APR1400-Z-J-EC-13001-NP
Revision 0

Safety I&C System for the APR1400

Revision 0

Non-Proprietary

February 2013

KEPCO KHNP

APR1400-Z-J-EC-13001-NP
Revision 0

Safety I&C System for the APR1400

Revision 0

Non-Proprietary

February 2013

KEPCO KHNP

Safety I&C System

for the APR1400

Revision 0

Non-Proprietary

February 2013

Revision History

Revision	Date	Page	Description
0	February 2013	All	Original Issue

ABSTRACT

This Topical Report provides the system description and the design process of the digital computer-based Safety I&C System which is intended to be used for Nuclear Regulatory Commission (NRC) Design Certification application of the APR1400.

This report is focused on the functional requirements, design features and software design process for the plant protection system (PPS), core protection calculator system (CPCS), engineered safety features –component control system (ESF-CCS) and qualified indication and alarm system – PAMI (QIAS-P). It includes the system's conformance to codes and standards, I&C system overview, safety I&C systems configuration and description, data communication network, software reliability, equipment qualification plan and equipment reliability analysis methodology.

This report also includes three appendices; Conformance to IEEE Std. 603-1991, Conformance to IEEE Std. 7-4.3.2-2003 and Conformance to ISG-04.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Acronyms and Abbreviations

AFAS	Auxiliary Feedwater Actuation Signal
AFW	Auxiliary Feedwater
AFWS	Auxiliary Feedwater System
AI	Analog Input
ALMS	Acoustic Leak Monitoring System
AMI	Accident Monitoring Instrumentation
ANS	American National Standard, American Nuclear Society
ANSI	American National Standards Institute
AO	Analog Output
AOO	Anticipated Operational Occurrence
APC-S	Auxiliary Process Cabinet – Safety
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
BDAS	Boron Dilution Alarm System
BISI	Bypassed and Inoperable Status Indication
BOP	Balance of Plant
BP	Bistable Processor
BTP	Branch Technical Position
CCC	Cross Channel Communication
CCF	Common - Cause Failure
CEA	Control Element Assembly
CEAC	CEA Calculator
CEDM	Control Element Drive Mechanism
CET	Core Exit Thermocouple
CGD	Commercial Grade Dedication
CI	Communication Interface
CIAS	Containment Isolation Actuation Signal
CIM	Component Interface Module
CIV	Containment Isolation Valve
COLSS	Core Operating Limit Supervisory System
COTS	Commercial Off-the-Shelf
CPIAS	Containment Purge Isolation Actuation Signal
CPC-CWP	CEA Withdrawal Prohibit by the CPCS
CPC(S)	Core Protection Calculator (System)
CPM	Control Panel Multiplexer
CPP	CEA Position Processor

CPU	Central Processing Unit
CRC	Cyclic Redundancy Checksum
CREVAS	Control Room Emergency Ventilation Actuation Signal
CS	Communication Section
CSAS	Containment Spray Actuation Signal
CVCS	Chemical Volume Control System
CWP	CEA Withdrawal Prohibit
D3	Diversity and Defense-in-Depth
DB	Database
DBE	Design-Basis Event
DCD	Design Control Document
DCN-I	Data Communication Network - Information
DCS	Data Communication System
DI	Digital Input
DIS	Diverse Indication System
DMA	Diverse Manual ESF Actuation
DNBR	Departure from Nucleate Boiling Ratio
DO	Digital Output
DPS	Diverse Protection System
DPRAM	Dual-Ported Random Access Memory
DRCS	Digital Rod Control System
DAS	Diverse Actuation System
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ENFMS	Ex-core Neutron Flux Monitoring System
EOP	Emergency Operation Procedure
EPRI	Electric Power Research Institute
ESCM	ESF-CCS Soft Control Module
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
ESF-CCS	Engineered Safety Features - Component Control System
FE	Function Enable
FHEVAS	Fuel Handling Area Emergency Ventilation Actuation Signal
FIDAS	Fixed In-core Detector Amplifier System
FMEA	Failure Modes and Effects Analysis
FOM	Fiber Optic Modem
FPD	Flat Panel Display

FPGA	Field Programmable Gate Array
FWCS	Feedwater Control System
GC	Group Controller
GDC	General Design Criteria
HDLC	High Level Data Link Control
HFE	Human Factors Engineering
HJTC	Heated Junction Thermocouple
HRA	Human Reliability Analysis
HSI	Human - System Interface
HVAC	Heating, Ventilation, and Air Conditioning
HW	Hardwired
ICC(M)	Inadequate Core Cooling (Monitoring)
ICIS	In-Core Instrumentation System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFPD	Information Flat Panel Display
I&C	Instrumentation and Control
IPS	Information Processing System
IRWST	In - Containment Refueling Water Storage Tank
ITA	Important to Availability
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
ITP	Interface and Test Processor
ITS	Important to Safety
IVMS	Internal Vibration Monitoring System
KHNP	Korea Hydro & Nuclear Power Co., Ltd.
LC	Loop Controller
LCL	Local Coincidence Logic
LCO	Limiting Condition of Operation
LDP	Large Display Panel
LOCA	Loss of Coolant Accident
LPD	Local Power Density
LPMS	Loose Parts Monitoring System
MCR	Main Control Room
MI	Minimum Inventory
MIL	Military Specifications

MSIS	Main Steam Isolation Signal
MSIV	Main Steam Isolation Valve
MTC	MTP/ITP Cabinet
MTP	Maintenance and Test Panel
NIMS	NSSS Integrity Monitoring System
NPCS	NSSS Process Control System
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
O&M	Operation & Maintenance
OM	Operator Module
PAMI	Post-Accident Monitoring Instrumentation
P-CCS	Process - Component Control System
PCS	Power Control System
PF	Penalty Factor
PI	Process instrumentation
PM	Processor Module
PLC	Programmable Logic Controller
PLCS	Pressurizer Level Control System
PPCS	Pressurizer Pressure Control System
PPS	Plant Protection System
PRA	Probabilistic Risk Analysis
PS	Processing Section
PVNGS	Palo Verde Nuclear Generating Station
PZR	Pressurizer
QAM	Quality Assurance Manual
QIAS-P	Qualified Indication and Alarm System - PAMI
QIAS-N	Qualified Indication and Alarm System - Non-safety
RAM	Random Access Memory
RCP	Reactor Coolant Pump
RCPSSSS	Reactor Coolant Pump Shaft Speed Sensing System
RCPVMS	Reactor Coolant Pump Vibration Monitoring System
RCS	Reactor Coolant System
RFI	Radio Frequency Interference
RG	Regulatory Guide
RH	Relative Humidity

RMS	Radiation Monitoring System
RO	Reactor Operator
ROM	Read Only Memory
RPCS	Reactor Power Cutback System
RPS	Reactor Protection System
RRS	Reactor Regulating System
RSC	Remote Shutdown Console
RSR	Remote Shutdown Room
RSPT	Reed Switch Position Transmitter
RT	Reactor Trip
RTM	Requirement Traceability Analysis
RTSG	Reactor Trip Switchgear
RTSS	Reactor Trip Switchgear System
SAFDL	Specified Acceptable Fuel Design Limit
SAT	Site Acceptance Test
SBCS	Steam Bypass Control System
SC	Safety Console
SCM(P)	Software Configuration Management (Plan)
SDD	Software Design Description
SDL	Serial Data Link
SDN	Safety System Data Network
SDOE	Secure Development and Operational Environment
SDP	Software Development Plan
SFC	Single-Failure Criterion
S/G	Steam Generator
SIAS	Safety Injection Actuation Signal
SInstP	Software Installation Plan
SIntP	Software Integration Plan
SMP	Software Management Plan
SODP	Shutdown Overview Display Panel
SOMP	Software Operation and Maintenance Plan
SPADES+	Safety Parameter Display and Evaluation System plus
SPDS	Safety Parameter Display System
SPM	Software Program Manual
SQAP	Software Quality Assurance Plan
SRDC	Safety-Related Divisional Cabinet
SRM	Staff Requirements Memoranda
SRP	Standard Review Plan
SRS	Software Requirement Specification

SSE	Safe Shutdown Earthquakes
SSP	Software Safety Plan
ST	Shunt Trip
STD	Standard
STP	Software Test Plan
STrngP	Software Training Plan
SVVP	Software Verification and Validation Plan
SVVR	Software Verification and Validation Report
S/W	Software
TCB	Trip Circuit Breaker
TCS	Turbine Control System
TMI	Three Mile Island
TO	Turbine Operator
TS	Technical Specification
TT	Turbine Trip
UV	Undervoltage
Vac	Volts-alternating current
VBPSS	Vital Bus Power Supply System
Vdc	Volts-direct current
V&V	Verification and Validation

1. PURPOSE

This Topical Report provides the system description and the design process of the digital computer-based safety I&C system, which is intended to be used for NRC Design Certification application of the APR1400.

2. SCOPE

This report describes the functional requirements, design features and software design process of the safety I&C system, particularly the plant protection system (PPS), core protection calculator system (CPCS), engineered safety features – component control system (ESF-CCS) and qualified indication and alarm system-PAMI (QIAS-P)

It includes the system's conformance to codes and standards, I&C system overview, safety I&C system configuration and design description, data communication network, software reliability, equipment qualification plan and equipment reliability analysis methodology.

This report also includes three appendices; Conformance to IEEE Std. 603-1991, Conformance to IEEE Std. 7-4.3.2-2003 and Conformance to ISG-04.

The envelope of this report does not include sensor inputs, ancillary trip systems or other safety I&C systems/equipments.

The diversity and defense-in-depth (D3) analysis is addressed in the Diversity and Defense-in-Depth Technical Report (Reference 1) and common-cause failure (CCF) analysis for the safety I&C systems coincident with design basis events (DBEs) is addressed in the CCF Coping Analysis Technical Report (Reference 5).

3. APPLICABLE CODES AND REGULATIONS

This section describes the compliance of the safety I&C systems with the applicable codes and regulations in effect as of December 31, 2012. The system's conformance to IEEE Std. 603-1991, IEEE Std. 7-4.3.2-2003 and NRC Interim Staff Guidance (ISG) DI&C-ISG-04, "Highly-Integrated Control Rooms – Communications Issues" are addressed in Appendix A, B and C of this report.

3.1. 10 CFR Part 50 and 52

a. 10 CFR 50.34(f)(2)(v), "Bypass and Inoperable Status Indication"

The indications of bypasses and inoperable status of the safety I&C systems are available on the operator module (OM), maintenance and test panel (MTP), qualified indication and alarm system - non-safety (QIAS-N) and information processing system (IPS) displays.

See compliance with Regulatory Guide (RG) 1.47 in Section 3.4.3 of this report.

b. 10 CFR 50.34(f)(2)(xii), "Auxiliary Feedwater System Automatic Initiation and Flow Indication"

The low steam generator (S/G) water level trip signal initiates a reactor trip when the measured water level in a S/G's downcomer region falls to a low preset value. Separate initiations are provided for the reactor protection system (RPS) and auxiliary feedwater actuation system (AFAS) to allow different setpoints for reactor trips and auxiliary feedwater actuations.

The AFAS continues to deliver auxiliary feedwater to the S/G until a preset water level has been reestablished. Manual actuation is provided to permit the operator to actuate the AFAS.

Auxiliary feedwater flow rate is displayed by using the IPS and diverse indication system (DIS).

c. 10 CFR 50.34(f)(2)(xiv), "Containment Isolation Systems"

The containment isolation actuation system (CIAS) is provided to mitigate the release of radioactive material during an accident by actuating the containment isolation valves (CIVs) which close the process lines penetrating the containment.

d. 10 CFR 50.34(f)(2)(xi), "Direct Indication of Relief and Safety Valves"
10 CFR 50.34(f)(2)(xvii), "Accident Monitoring Instrumentation"
10 CFR 50.34(f)(2)(xviii), "Instrumentation for Detection of Inadequate Core Cooling"
10 CFR 50.34(f)(2)(xix), "Instrumentation for Monitoring Plant Conditions Following Core Damage"

Specific functions to meet the Post-TMI requirements are described in the Design Control Document (DCD) Chapter 7.

e. 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants"

The safety I&C systems are installed in a mild environment and therefore this criteria is not applicable. This criteria is applicable to instrumentation that interfaces to this systems.

f. 10 CFR 50.55a(a)(1), "Quality Standards"

The Safety I&C systems are defined as Quality Class Q and Safety Class 3 according to ANSI/ANS-51.1-1983 (Reaffirmed 1988, Withdrawn 1998).

g. 10 CFR 50.55a(h), "Protection and Safety Systems"

The safety I&C systems are designed in accordance with the requirements of IEEE Std. 603-1991. Conformance to IEEE Std. 603-1991 is described in Appendix A of this report.

h. 10 CFR 50.62, "Requirements for Reduction of Risk from ATWS"

The diverse protection system (DPS) is designed to satisfy Anticipated Transient Without Scram (ATWS) requirements and described in the Diversity and Defense-in-Depth Technical Report (Reference 1). The DPS is diverse from the safety I&C systems.

i. 10 CFR 52.47(b)(1), "ITAAC for Standard Design Certification"

The Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) is described in the APR1400 DCD.

j. 10 CFR 50 Appendix A, "General Design Criteria for Nuclear Power Plants"

The safety I&C systems are designed in accordance with 10 CFR 50 Appendix A as described in Section 3.2.

k. 10 CFR 50 Appendix B. "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants"

The safety I&C systems are designed in accordance with 10 CFR 50 Appendix B.

l. 10 CFR Part 100, "Reactor Site Criteria"

The D3 coping analysis is performed to meet the acceptance criteria of fission product releases in accordance with 10 CFR Part 100 and the results are described in the CCF Coping Analysis Technical Report (Reference 5).

3.2. 10 CFR Part 50 Appendix A, General Design Criteria

a. GDC 1, "Quality Standards and Records"

The Quality Assurance Manual (QAM) conforms to the requirements of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants ".

b. GDC 2, "Design Bases for Protection Against Natural Phenomena"

The safety I&C systems are designated as Seismic Category I. The safety I&C systems are installed in the I&C equipment rooms or main control room (MCR) that provide protection against other natural phenomena, such as wind, tornado and flood.

c. GDC 4, "Environmental and Dynamic Effects Design Bases"

The safety I&C systems are located in mild environments (MCR or I&C equipment rooms). The MCR and I&C equipment rooms are designed to withstand the dynamic effects of missiles, pipe whipping or discharging fluids.

d. GDC 10, "Reactor Design"

The safety I&C systems contribute to reactor design margin by providing conservatism in setpoint calculations and fault-tolerant features. Uncertainties methodology is described in the Uncertainty Methodology and Application for Instrumentation (Reference 3) and setpoint methodology is described in the Setpoint Methodology for Plant Protection System (Reference 2).

e. GDC 13, "Instrumentation and Control"

The PPS consists of the RPS and the engineered safety features actuation system (ESFAS). The RPS is designed to monitor nuclear steam supply system's (NSSS) operating conditions and to initiate reliable and rapid reactor shutdown if monitored variables or combinations of monitored variables deviate from the permissible operating range to a degree where a safety limit may be reached. The ESFAS is designed to monitor plant variables and to actuate engineered safety features (ESF) systems during a DBE.

The ESF-CCS serves the functions of actuating ESFAS and executing component control through interfacing ESFAS portion of the PPS. It performs 2-out-of-4 voting logic for four channel ESFAS initiation signals derived from PPS and component control logic of ESF components.

The CPCS generates low departure from nucleate boiling ratio (DNBR) and high local power density (LPD) trip signals and sends them to the PPS.

The QIAS-P is to provide a continuous display of accident monitoring instrumentation (AMI) variables and an unambiguous indication of the approach to and the recovery from inadequate core cooling (ICC).

f. GDC 15, "Reactor Coolant System Design"

The PPS functions to mitigate the consequences in the event of an accident. Safety analyses show that the design limits for the reactor coolant pressure boundary are not exceeded in the event of any conditions stated in ANSI/ANS 51.1-1983, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants".

g. GDC 16, "Containment Design"

The PPS functions to mitigate the release of radioactive materials during an accident by actuating the CIVs which close the process lines penetrating the containment.

The PPS functions to actuate the containment spray actuation system (CSAS) which removes heat from the containment atmosphere. The heat removal process results in reduction of containment temperature and pressure below the design values during and following an accident.

h. GDC 19, "Control Room"

The MCR safety console (SC) is equipped with manual reactor trip initiation switches, manual ESF actuation switches and OMs shared by PPS and CPCS. Monitoring for safe operation is implemented with the QIAS-P, QIAS-N and IPS displays. Also, the DPS, DIS and diverse manual ESF actuation (DMA) switches are provided against CCFs in the safety I&C systems coincident with DBEs.

i. GDC 20, "Protection System Functions"

The safety I&C systems functions are described in Section 4 of this report.

j. GDC 21, "Protection System Reliability and Testability"

The safety I&C systems are designed to provide high functional reliability and in-service testability. The protection system is designed to comply with the requirements of IEEE 603-1991 and other standards endorsed by RGs. No credible single failure will result in loss of the protection function. The protection channels are independent each other with respect to wire routing, sensor mounting and power supply.

Each channel of the protection system, including the sensors, up to the reactor trip switchgear system (RTSS) and ESF actuation devices, is capable of being checked during reactor operation. Process sensors of each channel in the protection systems are checked in the IPS through comparison of the redundant process sensor values using the discrete indications and alarms in the MCR.

To minimize inadvertent actuation of an ESF system or an inadvertent reactor trip, the protection systems utilize a 2-out-of-4 coincidence voting logic. In addition, the channel under testing is bypassed so that the voting logic converts to a 2-out-of-3 logic. This allows periodic testing without loss of the protective functions during power operation.

k. GDC 22, "Protection System Independence"

The safety I&C systems conform to the independence requirements of IEEE 603-1991. Four independent measurement channels with sensors, sensor power supplies, signal conditioning units, and bistable trip functions are provided for each protective parameter monitored by the protection systems except for the control element assembly (CEA) position sensors which are two-fold redundant.

Power to the protection system channels is provided by independent vital power supply buses.

l. GDC 23, "Protection System Failure Modes"

The PPS trip channels are designed to fall into a safe state in the event of loss of power supply. A failure is assumed to occur in only one channel (i.e., a single failure). This channel can be placed into bypass mode which places the RPS/ESFAS local coincidence logic into a 2-out-of-3 configuration which retains the coincidence of two for trip initiation.

Failure modes and effects analysis (FMEA) for safety I&C systems is described in the APR1400 DCD.

m. GDC 24, "Separation of Protection and Control System"

Complete electrical, physical and communication isolations are maintained between redundant safety channels, and between the safety system and non-safety system.

n. GDC 25, "Protection System Requirements for Reactivity Control Malfunctions"

Shutdown of the reactor is accomplished by opening of the RTSS circuit breakers which interrupt power to the control element drive mechanism (CEDM) coils. Actuation of the circuit breakers is independent of any existing control signals. The safety I&C systems are designed such that specified acceptable fuel design limits (SAFDLs) are not exceeded for any single malfunction of the reactivity control systems, including the withdrawal of a single full- or part-strength CEA.

o. GDC 29, 'Protection Against Anticipated Operational Occurrences"

Plant events, designated in ANSI/ANS 51.1-1983, have been carefully considered in the design of the protection and reactivity control systems.

Consideration of redundancy, independence and testability in the design, coupled with careful component selection, overall system testing and adherence to detailed quality assurance requirements assure that safety functions are accomplished in the event of DBEs.

3.3. Commission Paper and NUREG Reports

3.3.1 SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactors", II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems"

Analyses and design features for D3 for the safety I&C systems are provided in accordance with SECY 93-087, II.Q, as referenced by NUREG-0800.

The DPS automatically initiates reactor trip on high containment pressure to assist the mitigation of the effects of a postulated CCF of the safety I&C systems, concurrent with a main steam line break inside containment. The DPS also automatically initiates safety injection actuation signal (SIAS) on low pressurizer (PZR) pressure in case of loss of coolant accident with CCF of the safety I&C systems.

The DMA switches are provided to allow manual control capability to support system level ESF actuation in the event of a postulated CCF of the safety I&C systems.

The DIS displays position 4 variables in the event of a postulated CCF of the safety I&C systems.

Compliance to SRM on SECY 93-087 and diverse I&C system design features are addressed in the Diversity and Defense-in-Depth Technical Report (Reference 1).

The detailed CCF analysis methodology and the results are described in the CCF Coping Analysis Technical Report (Reference 5).

3.3.2 NUREG-0737, "Clarification of TMI Action Plan Requirements," 1980

The QIAS-P displays variables indicating ICC in accordance with Section II.F.II "Instrumentation for detection of inadequate core cooling" of NUREG-0737.

3.3.3 NUREG-0737, Supplement 1, "Clarification of TMI Action Plan Requirements: Requirements for Emergency Response Capability", 1982.

Safety parameter display and evaluation system+ (SPADE+) displays variables and information on IPS in accordance with Section I.D.2 "Plant Safety Parameter Display Console" of NUREG-0737 Supplement 1.

3.4. Regulatory Guides

3.4.1 Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions", Rev.0

The safety I&C systems conform to the guidance of RG 1.22 as follows:

a. Provisions are made to permit periodic testing of the complete safety I&C systems with the reactor operating at power or when shutdown.

b. The provisions are incorporated in the testing of the PPS, from sensor to actuated device, including the RTSS and the ESF-CCS.

c. The manual testing is interlocked to prevent a trip in more than one redundant channel simultaneously.

d. When a channel is bypassed for manual testing, the bypass status is indicated in the MCR.

e. ESF actuation devices which cannot be tested during reactor operation are tested during reactor shutdown.

3.4.2 Regulatory Guide 1.29, "Seismic Design Classification," Rev. 4

The seismic design classification is designated as Seismic Category I or non-Seismic Category I depending on the functional and/or physical integrity requirements of the APR1400 plant I&C systems.

3.4.3 Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems", Rev. 1

The bypassed and inoperable status indication (BISI) is processed by the IPS and displayed on the large display panel (LDP) and information flat panel display (IFPD). The BISI provides system level indication of deliberately introduced inoperability of protection system for which is required for safe operation of the plant. The system level alarms are actuated when a component actuated by a protection system is bypassed or deliberately rendered inoperable.

3.4.4 Regulatory Guide 1.53, "Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems", Rev. 2- endorses IEEE Std. 379-2000 (Reaffirmed 2008)

Instrumentation for the safety I&C systems conforms to the requirements of IEEE 379-2000 "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems," as endorsed by RG 1.53.

The safety I&C systems are designed to assure both the reactor safety and prevention of a spurious reactor trip. Safety is assured by design in accordance with IEEE Std. 603-1991. The prevention of spurious trip due to single failure is assured by 2-out-of-4 voting logic in conjunction with a channel bypass design in accordance with IEEE Std. 379-2000.

3.4.5 Regulatory Guide 1.62, "Manual Initiation of Protection Action", Rev. 1

Conformance to RG 1.62 is as follows:

a. Each of the RPS and ESFAS function can be manually actuated.

b. Manual initiation of a protective action is provided at the system level.

c. Manual switches are located on the MCR SC and RTSS. Some ESF functions also have manual actuation at the remote shutdown console (RSC).

d. The amount of equipment common to the manual and automatic initiation paths is kept to a minimum, usually just the actuation devices. No single credible failure in the manual, automatic, or common portions of the protective system prevents initiation of a protective action by manual or automatic means.

e. Manual initiation requires a minimum of equipment consistent with the needs of a, b, c, and d above.

3.4.6 Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems", Rev. 3 - endorses IEEE Std. 384-1992

The instrumentation for the safety-related electrical systems conforms to the requirements of IEEE 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," as endorsed by RG 1.75. A discussion of the physical independence is provided below which describes the compliance with Section 5.6 of IEEE 603-1991 and GDC 21.

The PPS is divided into four channels which are physically located in different geographic fire zones. This provides the separation and independence necessary to meet the requirements of Section 5.6 of IEEE 603-1991.

The independence and separation of redundant Class 1E circuits within and between the PPS channels or ESF-CCS channels is accomplished primarily through the use of fiber-optic technology and barriers or conduits. The optical technology ensures that no single credible electrical fault in PPS and ESF-CCS channel can prevent the circuitry in any other redundant channel from performing its safety function.

The ESF-CCS cabinets provide separation and independence for the 2-out-of-4 actuation and component control logic of the redundant ESF system trains. Each train's component control logic is contained in a separate cabinet. The redundant cabinets are physically separated from each other by locating them in separated zones.

Protection system's analog and digital signals sent to non-Class 1E systems for status monitoring, alarm and display (e.g., IPS, QIAS-N) are isolated from the non-safety system. Fiber-optic isolation and other techniques are used to ensure no credible failures on the non-Class 1E side of the isolation device will affect the PPS side and that independence of the PPS is not jeopardized.

3.4.7 Regulatory Guide 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," Rev. 4- endorses IEEE Std. 497-2002

QIAS-P processes and displays variables for Types A/B/C, of which Type A variables are displayed using conventional analog indicators, defined in Section 4.0 of IEEE 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations", as augmented by RG 1.97. QIAS-N processes and displays variables for Types A/B/C/D/E.

3.4.8 Regulatory Guide 1.100, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants," Rev. 3 – endorses IEEE Std. 344-2004 (Reaffirmed 2009)

The safety I&C systems are designated as Seismic Category I to withstand the cumulative effects of five 1/2 safe shutdown earthquake (SSEs) followed by one SSE without loss of safety functions or physical integrity.

3.4.9 Regulatory Guide 1.105, "Setpoints for Safety-Related Instrumentation", Rev. 3 - endorses Part 1 of ISA-S67.04-1994

The generation of safety system setpoints conforms to ISA-S67.04-1994, "Setpoints for Nuclear Safety Related Instrumentation Used in Nuclear Power Plants."

The environment considered when determining errors is the most detrimental realistic environment calculated or postulated to exist until the worst case time of the required reactor trip or ESF system actuation. This environment may be different for different events analyzed. For the setpoint calculation, the accident environment error calculation for process equipment uses the environmental conditions up to the longest required time of trip or actuation that results in the largest errors, thus providing additional conservatism to the resulting setpoints.

For all temperature and pressure setpoints, the trip will be initiated at a point that is not at saturation for the equipment. For level setpoints, no analysis setpoint is within 5% of the ends of the level span.

Uncertainties and setpoint methodology is described in the Uncertainty Methodology and Application for Instrumentation (Reference 3) and Setpoint Methodology for Plant Protection System (Reference 2).

3.4.10 Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems", Rev. 3 endorses IEEE Std. 338-1987

The safety I&C systems are designed so that they can be periodically tested in accordance with the criteria of IEEE 338-1987, "IEEE Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems", as endorsed by RG 1.118.

The system is periodically and routinely tested to verify its operability. A complete channel can be tested without causing a reactor trip or ESF system actuation, and without affecting system operability or availability. Overlap in the RPS and ESFAS channel tests is provided to assure that the entire channel is functional. The testing scheme is described in Section 4.2.2 of this report.

When any one channel in the PPS portion is being tested, the remaining three channels still provides a coincidence logic to effect actuation via the RTSS and the ESF-CCS.

3.4.11 Regulatory Guide 1.151, "Instrument Sensing Lines," Rev.1

Conformance to RG 1.151 is described in Section 1.8 of APR1400 DCD.

3.4.12 Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants", Rev. 3 - endorses IEEE Std. 7-4.3.2-2003

The methods for specifying, designing, implementing, verifying, validating and maintaining the safety I&C systems software conform to IEEE Std. 7-4.3.2-2003, as augmented by RG 1.152. Section 5 of this report describes the life cycle process for the safety I&C systems application software.

3.4.13 Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Rev. 1- endorses IEEE Std. 1012-1998 and IEEE Std. 1028-1997

The software verification, validation, reviews and audits process for the safety I&C systems conform to IEEE Std. 1012-1998 and IEEE Std. 1028-1997 endorsed by RG 1.168. The Verification & Validation (V&V) plan, process and activities are described in Section 5 of this report.

3.4.14 Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", Rev. 0 - endorses IEEE Std. 828-1990 and IEEE Std. 1042-1997

The software configuration management process for the safety I&C systems conforms to IEEE Std. 828-1990 and IEEE Std. 1042-1997 endorsed by RG 1.169. The configuration plan and methods are described in Section 5 of this report.

3.4.15 Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", Rev. 0 - endorses IEEE Std. 829-1983

The software test documentation for the safety I&C systems conforms to IEEE Std. 829-1983 endorsed by RG 1.170. The test documentation is described in Section 5 of this report.

3.4.16 Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", Rev. 0 - endorses IEEE Std. 1008-1987

The software unit testing process for the safety I&C systems conforms to IEEE Std. 1008-1987 endorsed by RG 1.171. The unit testing approaches are described in Section 5 of this report.

3.4.17 Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", Rev. 0 - endorses IEEE Std. 830-1993

The software requirements specifications for the safety I&C systems are developed according to IEEE Std. 830-1993 endorsed by RG 1.172.

3.4.18 Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", Rev. 0 - endorses IEEE Std. 1074-1995

The software life cycle model for the safety I&C systems is consistent with IEEE Std. 1074-1995 endorsed by RG 1.173. The software life cycle activities are described in Section 5 of this report.

3.4.19 Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control", Rev. 1- endorses MIL Std. 461E-1999, IEEE Std. 1050-1996, IEC 61000-Parts 3, 4 and 6, IEEE Std. C62.41-1991 and IEEE Std. C62.45-1992

The safety I&C systems equipment are qualified according to the EMI/RFI requirements of RG 1.180 and the endorsed standards. The equipment qualification plan is described in Section 6 of this report.

3.4.20 Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)", Rev. 0

The APR1400 DCD including this Topical Report is prepared in accordance with the guidance described in RG1.206 together with NUREG-0800 Standard Review Plan (SRP) in order for NRC to evaluate and confirm the safety determination.

3.4.21 Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Instrumentation and Control Systems in Nuclear Power Plants", Rev. 0 - endorses IEEE Std. 323-2003 (Reaffirmed 2008)

The safety I&C systems equipment are qualified to the requirements of IEEE Std. 323-2003, as endorsed by RG 1.209. Since the equipment is located in the MCR and/or I&C equipment rooms, there is no change in the environment due to plant accidents. The safety I&C

systems equipment are tested and analyzed to meet the mild environmental qualification requirements.

3.5. Branch Technical Positions

3.5.1 BTP 7-1 Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System

3.5.2 BTP 7-2 Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines

3.5.3 BTP 7-3 Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service

3.5.4 BTP 7-4 Guidance on Design Criteria for Auxiliary Feedwater Systems

3.5.5 BTP 7-5 Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors

3.5.6 BTP 7-6 Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

Compliance to Branch Technical Position (BTP) 7-1 through BTP 7-6 is described in the APR1400 DCD Table 7.1-2

3.5.7 BTP 7-8 Guidance for Application of Regulatory Guide 1.22

Provisions are made to permit periodic testing of the complete safety I&C systems for all functions with the reactor operating at power or when shutdown

3.5.8 BTP 7-9 Guidance on Requirements for Reactor Protection System Anticipatory Trips

All non-safety system is isolated from the safety system to prevent adverse effect. Safety functions have higher priority than all non-safety functions. Analysis demonstrates that

failures of non-safety system do not result in plant conditions that are outside the boundary of the safety analysis.

3.5.9 BTP 7-10 Guidance on Application of Regulatory Guide 1.97

The QIAS-P and conventional indicators for Type A variables comply with RG 1.97 Revision 4.

3.5.10 BTP 7-11 Guidance on Application and Qualifications of Isolation Devices - endorses IEEE Std. 472, ANSI Std. C62.36, ANSI Std. C62.41, ANSI Std. C62.45

The isolation devices are qualified in accordance with these standards.

3.5.11 BTP 7-12 Guidance on Establishing and Maintaining Instrument Setpoints

Uncertainty and setpoint calculations are described in the Uncertainty Methodology and Application for Instrumentation (Reference 3) and Setpoint Methodology for Plant Protection System (Reference 2).

3.5.12 BTP 7-13 Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

The methods used for periodically verifying the accuracy and response time of RTDs complies with this standard. The method is described in the APR1400 DCD Chapter 7.

3.5.13 BTP 7-14 Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems -endorses IEEE Std. 730

See Sections 3.4.13 through 3.4.18 of this report for compliances.

3.5.14 BTP 7-17 Guidance on Self-Test and Surveillance Test Provisions

See Sections 3.2.j, 3.4.1 and 3.4.10 of this report for compliances.

3.5.15 BTP 7-18 Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

The safety I&C systems are based on a common programmable logic controller (PLC) platform which are manufactured in accordance with 10 CFR 50 Appendix B. The hardware is qualified to satisfy the nuclear requirements such as environmental, seismic, and EMI/RFI qualifications. The software is designed, verified and validated with codes and industry standards for software development and V&V process endorsed by NRC.

3.5.16 BTP 7-19 Guidance on Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems

Compliance to this standard is addressed in the Diversity and Defense-in-Depth Technical Report (Reference 1).

3.5.17 BTP 7-21 Guidance on Digital Computer Real-Time Performance

Real-time performance is determined by performing response time analysis for all safety functions. An analysis for each function is performed, which demonstrates the actual system response time is less than the response time requirements. The specific response time requirements are described in the Setpoint Methodology for Plant Protection System (Reference 2).

3.6. Interim Staff Guidance

3.6.1 DI&C-ISG-04, Digital Instrumentation and Control, Highly-Integrated Control Rooms – Communication Issues

The compliance to ISG-04 is addressed in Appendix C of this report.

4. I&C SYSTEM DESCRIPTION

4.1. Overall I&C System

As shown in Figure 4.1-1, the APR1400 I&C system consists of the safety systems, control & monitoring system, diverse actuation system and human-system interfaces (HSI) in the MCR and remote shutdown room (RSR).

The I&C system uses full digital technology, however the limited hardware switches are used to meet the safety system design criteria in IEEE Std. 603-1991 and analysis results of the D3.

The safety systems are based on a common PLC platform which has been dedicated for nuclear safety systems. The components of the safety system are qualified to satisfy the nuclear requirements such as environmental, seismic, and EMI/RFI qualifications. The safety system software is designed, verified and validated with industry standard software development and V&V process endorsed by the NRC. The safety systems implemented on the common PLC platform consist of the PPS, ESF-CCS, CPCS and QIAS-P. The QIAS–N is also implemented on the common PLC platform even though it is a non-safety system, because it displays the plant's important parameters and maintains diversity from the IPS. Also the control panel multiplexer (CPM) and interface and test processor (ITP) use the common PLC platform.

Most of the non-safety I&C systems are implemented in a distributed control system based common platform which has been proven by operating experiences from the nuclear industry as well as other industries. The DCS supports component-level control, automatic process control, and high-level group control. The DCS is designed in a redundant and fault-tolerant architecture to achieve high reliability and not to allow the failure of a single component to cause spurious plant trip. The non-safety systems implemented in the DCS are the power control system (PCS), NSSS process control system (NPCS), and process–component control system (P-CCS). However the DPS and DIS use a non-software based field programmable gate array (FPGA) platform which is diverse from PLC and DCS.

There are systems which are not installed in a common I&C platform. They have their unique hardware and fulfill the specific system design requirements. These non-standard systems typically include the ex-core neutron flux monitoring system (ENFMS), NSSS integrity monitoring system (NIMS), auxiliary process cabinet – safety (APC-S) and component interface module (CIM).

The IPS consists of networking equipment, computer servers, flat panel displays (FPDs) and peripherals to provide the operator with the plant information and soft control for non-safety control components.

The plant-wide data networks are composed of safety system data networks (SDNs) and non-safety networks. The SDN is independent and diverse from the non-safety network. The non-safety data communication network-information (DCN-I) utilizes different communication hardware, software and communication protocol from the SDN.

The I&C architecture satisfies the independence, separation and diversity requirements as follows:

- Each of the safety systems is functionally, physically and electrically independent from each other to meet the single failure criteria.
- A safety channel does not receive any information or signals originating from another safety channel or non-safety division to perform its safety function except the voting logic.

- The data communication networks for the safety system and the non-safety system are independent and diverse from each other. There is no potential for the deterministic cyclic processing of the safety function to be disrupted by any data communication. One way communication from safety systems to non-safety systems and buffering circuit using dual port memory are commonly used to prevent endangering the safety function.
- The DPS is diverse from the protection systems such as safety I&C systems in aspects of trip mechanism, hardware and software.
- In addition to the DPS, the hardwired DMA switches and the DIS are provided on the MCR SC to cope with CCF of the safety I&C systems.

4.1.1. Protection and Safety Monitoring Systems

4.1.1.1. Plant Protection System

The plant protection system (PPS) consists of four redundant channels that perform the necessary bistable, coincidence, initiation logic, maintenance and test function.

The PPS initiates reactor trip and ESF actuation functions when required by the plant conditions. To detect such conditions, the system utilizes measurements of the reactor core, reactor coolant system, main steam system and containment building parameters.

Each PPS channel receives the process and discrete signals directly from field sensors or via the APC-S, ENFMS and CPCS. The PPS provides the reactor trip signals to the RTSS using hardwired cables and ESFAS initiation signals to the ESF-CCS via fiber optic serial data links (SDLs).

4.1.1.2. Engineered Safety Features - Component Control System

The ESF-CCS, which comprises four independent channels for the NSSS and two independent channels for balance of plant (BOP), consists of group controller (GC), loop controller (LC), gateway, multiplexer, MTP, ITP and HSI that perform the necessary coincidence, component control logic and associated soft control function. The MTP and ITP are shared with PPS, CPCS and QIAS-P.

The ESF-CCS serves the functions of actuating ESFAS and executing component control through interfacing ESFAS portion of the PPS. It performs 2-out-of-4 voting logic for four-channel ESFAS initiation signals derived from PPS and component control logic of ESF components.

The manual ESFAS initiation signals are sent from the SC in the MCR to the ESF-CCS via the CPM.

4.1.1.3. Core Protection Calculator System

The CPCS has four redundant channels that compute the DNBR and LPD values using process values, reactor coolant pump (RCP) speed, CEA position and ex-core neutron flux.

The CPCS compares the DNBR and LPD values against setpoints to determine if fuel design limits are exceeded. When these values reach the setpoints, a trip signal is transmitted to the PPS using hardwired cables.

4.1.1.4. Qualified Indication and Alarm System - PAMI

The QIAS-P, which has two independent channels A and B, comprises the common PLC platform for the safety system. The qualified FPDs and processor unit for the QIAS-P are installed on the MCR SC.

The QIAS-P provides a continuous and dedicated display of AMI parameters specified in RG 1.97 Rev.4, Types B and C variables and the inadequate core cooling monitoring (ICCM) variables. Type A variables are displayed using conventional indicators. It receives plant parameters from the safety I&C systems via SDN, APC-S via hardwired interface and process instrumentation directly.

It transmits the sensor signals and their calculated variables to the IPS and QIAS-N through the MTP and ITP respectively.

4.1.1.5. Auxiliary Process Cabinet - Safety

The APC-S consists of four redundant channels designated as Class 1E. It receives safety-related sensor signals and distributes them to the PPS, CPCS, ESF-CCS, QIAS-P and non-safety systems (i.e., DIS) via hardwired interfaces.

It includes signal conditioning/splitting equipment and the associated power supplies for sensor input. Qualified isolation devices are provided within the APC-S to interface safety signals to the non-safety systems.

4.1.1.6. Ex-core Neutron Flux Monitoring System

The ENFMS provides a means to measure reactor power level by monitoring the neutron flux leakage from the reactor vessel for reactor control, protection and information display.

The ENFMS consists of four redundant safety channels and two redundant startup/control signal processing drawers. The startup/control signal processing drawers are independent from the four safety channels through the qualified isolation devices.

4.1.1.7. Component Interface Module

The CIM is a non-software based Class 1E module for safety critical component control. Based on its non-software design, it is not considered in the potential of software CCF. The CIM receives component control signals from the safety system (ESF-CCS) and DPS and arbitrates the signal to the plant component according to a user selectable priority (i.e., safety system priority or component state priority). In addition, the CIM receives DMA signal that is configured as one of input signals in priority logic.

4.1.1.8. Reactor Trip Switchgear System

The RTSS consists of four channels. The RTSS is designed as Class 1E. The RTSS receives the reactor trip signals from PPS through hardwired cable. The RTSS disconnects the power to digital rod control system (DRCS) for dropping CEAs into the reactor core by RPS signals from PPS or manual reactor trip signals from MCR or RSR.

4.1.2. Control and Monitoring System

4.1.2.1. Power Control System

The PCS integrates control systems that are designed to control the reactor power level, which includes the reactor regulating system (RRS), reactor power cutback system (RPCS) and DRCS.

The RRS/RPCS logic and DRCS cabinets include the redundant DCS controllers with associated I/O.

4.1.2.2. NSSS Process Control System

The NPCS consists of the PZR pressure control system (PPCS), PZR level control system (PLCS), feedwater control system (FWCS), steam bypass control system (SBCS), boron dilution alarm system (BDAS), and single control loops of the chemical and volume control system (CVCS).

The NPCS is installed as a part of the P-CCS.

4.1.2.3. Process - Component Control System

The P-CCS is designed to control non-safety related components such as pumps, valves, heaters and fans. The P-CCS performs data acquisition from field instruments and discrete/continuous controls, and provides process variables and their status information to the IPS and QIAS-N for plant monitoring.

Standardized component control logic and I/O interfaces are provided for the various types of components to be controlled. Manual operator controls for the P-CCS are performed through the soft control display on the IFPD driven by the IPS.

4.1.2.4. Fixed In-core Detector Amplifier System

The fixed in-core detector amplifier system (FIDAS) monitors the fixed in-core neutron detector current signals, performs the necessary signal conversion to engineering unit values and transmits them to the IPS. The IPS uses these signals for the core operating limit supervisory system (COLSS) to estimate the gross power distribution and thermal margin in the core, and fuel burn-up in each fuel assembly.

Neutron flux in the reactor core is measured by the fixed in-core neutron. Detectors are spaced radially and axially in sufficient numbers to permit representative flux mapping of the entire core.

4.1.2.5. Qualified Indication and Alarm System - Non-safety

The QIAS-N is a single channel indication and alarm system that supports continuous plant operation if the IPS is unavailable. It provides the information required for emergency operating procedure (EOP) execution, safe shutdown and critical operator action. The QIAS-N also provides RG 1.97 Types A, B, C, D and E variables.

It receives channelized information from the four safety channels via their ITPs.

The QIAS-N comprises the common PLC platform for the safety system. The QIAS-N HSI is provided by the qualified FPDs on the SC.

4.1.2.6. NSSS Integrity Monitoring System

The NIMS detects selected conditions which indicate a deterioration or which could lead to a deterioration of the RCS pressure boundary.

The system consists of internal vibration monitoring system (IVMS), acoustic leak monitoring system (ALMS), loose parts monitoring system (LPMS), and RCP vibration monitoring system (RCPVMS).

4.1.2.7. Information Processing System

The IPS is a computer based data processing system and HSI system that serves to provide operational means for control and monitoring of the plant. It consists of networking equipment and network, along with alarm server, application program server, data base (DB) server, data link server and IFPD installed in operator consoles. The information is derived from other I&C systems and self-contained algorithms called application programs.

The IPS HSI provides the operator with main HSI resources including process mimic displays, alarms, and historical data access. It is designed to enhance overall plant operation, availability and efficiency. Also it represents the soft control pages for manual component controls. The soft control of the IPS HSI is used for control associated with P-CCS controllers directly attached to the non-safety DCS platform network. The IPS HSI also interfaces to the EFS-CCS soft control module (ESCM) to send safety component selection information.

4.1.3. Diverse Actuation System

The detailed design description for diverse actuation system (DAS) is described in the Diversity and Defense-in-Depth Technical Report (Reference 1).

4.1.3.1. Diverse Protection System

The DPS is designed to mitigate the effects of ATWS event characterized by an anticipated operational occurrence (AOO) followed by a failure of the reactor trip portion of the protection system. In addition, the DPS is designed to include a function to assist in the mitigation of the effects of a postulated CCFs of the safety I&C system.

PZR pressure and containment pressure is respectively monitored by a bistable comparator to generate a reactor trip signal to each channel whenever a pressure exceeds a predetermined setpoint. The DPS automatically initiates auxiliary feedwater when the S/G level falls below a predetermined value. The DPS also initiates safety injection actuation when PZR pressure decreases below a predetermined value.

The DPS also automatically initiates a turbine trip (TT). The TT signal is generated from the DPS when the power to the DRCS is interrupted (i.e., as a result of a reactor trip signal generated in the PPS or DPS). When the DRCS undervoltage signal is transmitted to the DPS, the DPS generates the TT signal to the turbine control system (TCS).

Figure 4.1-2 shows the design concept of diversity between the protection system and the DPS.

4.1.3.2. Diverse Indication System

The DIS is a single channel of non-safety-related equipment to meet the NRC's display requirements for Point 4 on diversity and defense-in-depth for the safety I&C systems. The DIS is diverse from the safety I&C system.

The DIS provides plant operators with the following information that are not subject to CCF in the common PLC platform because the displays are independent and diverse from the safety I&C system.

- Inadequate core cooling monitoring information
- Part of AMI parameter information
- Emergency operation-related variables

4.1.3.3. Diverse Manual ESF Actuation Switches

The DMA switches are composed with conventional switches on the MCR SC for system level manual actuation of the ESF components, which is required for coping with CCF in safety I&C systems.

The DMA switches are independent and diverse from the manual and automatic logic functions performed by the safety I&C systems. The DMA signals are hardwired to CIM in the safety system architecture to the lowest practical level.

4.1.4. Human-System Interfaces

The HSI is designed in accordance with the advanced control design approach based on compact operator console using the soft control and distributed digital control system. The compact operator console based HSI provides a convenient operating environment to facilitate display of plant status information for the operator such that the operability can be improved by reducing human error to a great extent. And the HSI has sufficient diversity to demonstrate defense-in-depth protection against CCF of the distributed control system.

The HSI comprises the following operating facilities to support the operating staff for efficient and safe plant operation.

- Compact workstation-based operator consoles
- A LDP for display of overall plant operational and safety assessment data
- A SC for maintaining the plant in safe condition, which is functionally independent of the operator console

The operator console design uses multiple identical and redundant compact workstations. Each console allows access to all information and controls necessary for one operator to monitor and control all processes associated with nuclear plant operation and safety. Each operator console comprises four IFPDs, four ESCMs and pointing devices. The FPDs provide plant operating status information to the operator via graphical flow diagrams, alarm displays, plant summary displays, computerized procedures and non-safety soft control.

One set of channelized four ESCM FPDs also is installed on each operator console to provide manual control capability for safety component control.

The LDP continuously displays spatially dedicated information that provides the status of the plant critical safety functions, plant operation mode, key operating parameters and status, trend displays, etc. In addition to providing an overview and safety information, the LDP provides fixed indication of high priority alarms via alarm tiles and incorporates a variable display Section to support operating goals in progress.

A SC is located in the left side of the MCR. Hardwired safety-related fixed position controls are provided on the SC for manual actuation of the safety systems. Hence the MCR operators can still mitigate the accident and maintain the plant in safe condition using the SC in the unlikely event where all operator consoles have failed. OMs for PPS/CPCS and FPDs for QIAS-P, QIAS-N and DIS are also provided on the SC.

DMA switches and DIS are installed on the SC to provide diverse manual control and indication.

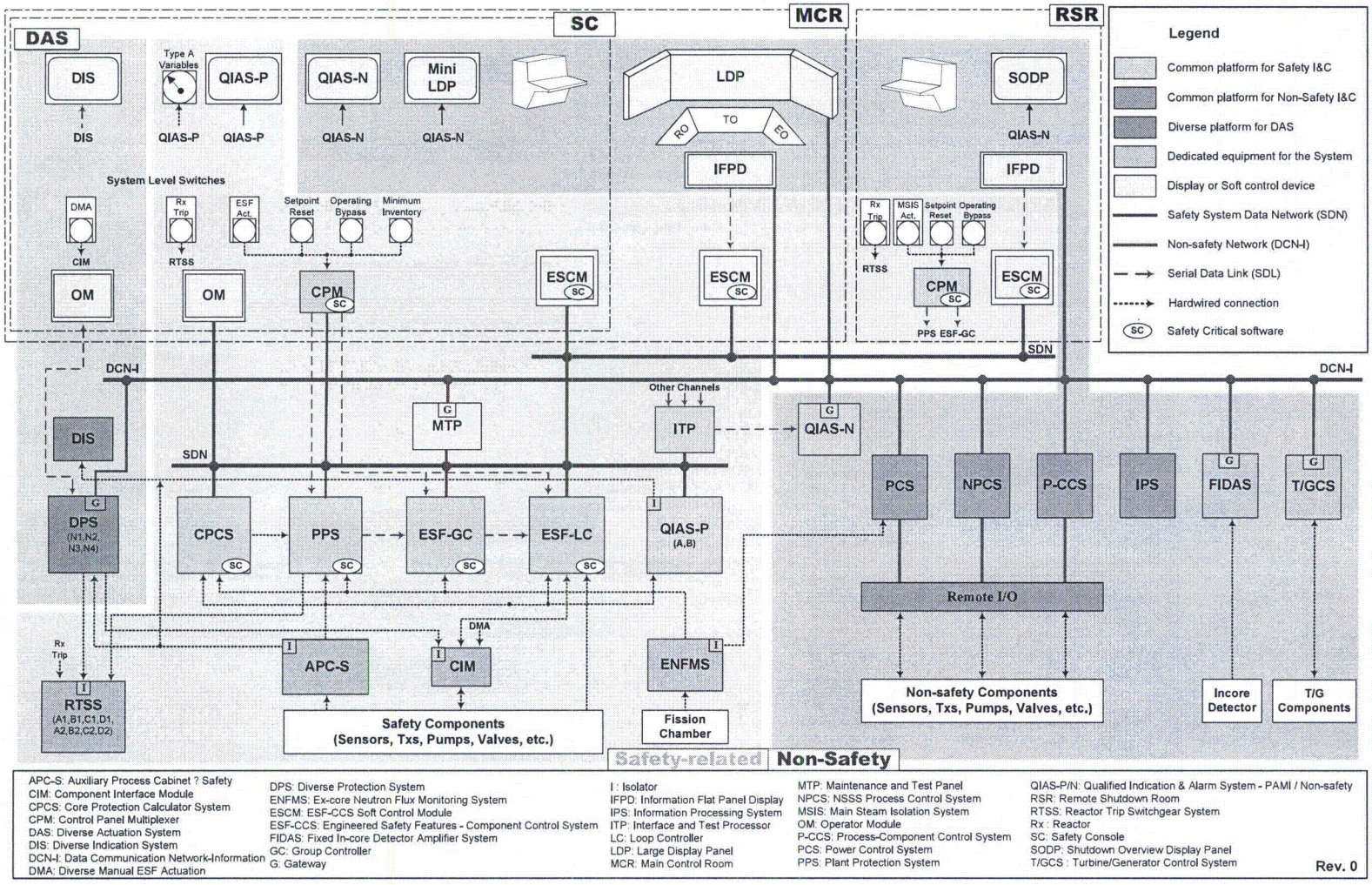


Figure 4.1-1 APR1400 I&C System Overview Architecture

TS

Figure 4.1-2 Diversity Design Concept between Protection System and Diverse Protection System

4.2. Plant Protection System

4.2.1. Functions

The PPS generates signals to actuate reactor trip (RT) and ESF automatically whenever monitored process variables reach predefined limits. It is also equipped with means for manual initiation of each protective action.

The PPS provides status outputs for operator monitoring and receives manually entered inputs for limited operator intervention in the automatic RT and ESF actuation, such as an operating bypass and setpoint reset.

The PPS provides alarms and, in some cases limiting signals to control systems, whenever the selected plant process parameters approach the predetermined levels where plant protection would be required.

The PPS has a test capability for determining system operability and hardware diagnostic testing.

The PPS comprises two portions such as the reactor protection system (RPS) and ESFAS shown in Figure 4.2-1. Table 4.2-1 shows the plant condition to cause reactor trip and/or each ESFAS initiation function.

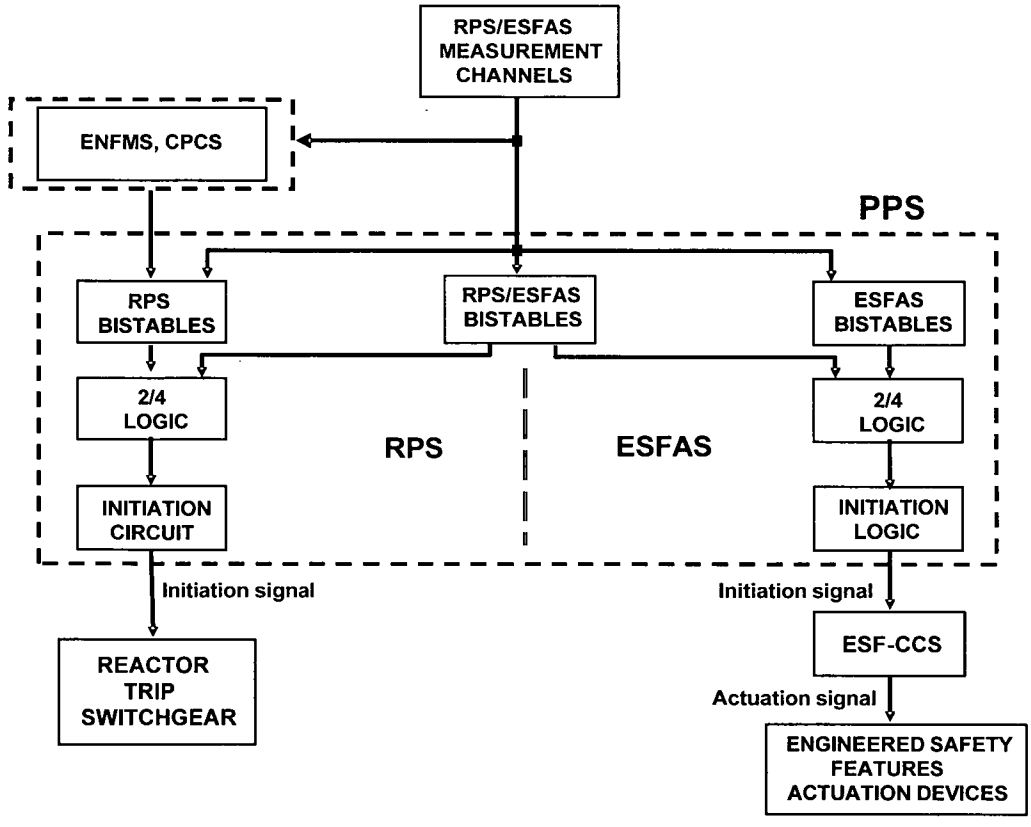


Figure 4.2-1 PPS Basic Functional Block Diagram

Table 4.2-1 Summary of RPS and ESFAS Initiation Function

Trip Parameter	RPS	ESFAS	Input from
Variable Over Power	RT		ENFMS
High Logarithmic Power Level	RT		ENFMS
High Local Power Density (LPD)	RT		CPCS
Low Departure from Nucleate Boiling Ratio (DNBR)	RT		CPCS
High PZR Pressure	RT		APC-S
Low PZR Pressure	RT	SIAS, CIAS	APC-S
High S/G 1&2 Level	RT	MSIS	APC-S
Low S/G 1&2 Level	RT	AFAS	APC-S
Low S/G 1&2 Pressure	RT	MSIS	APC-S
Low Reactor Coolant Flow	RT		APC-S
High Containment Pressure	RT	MSIS, CSAS	APC-S
High High Containment Pressure		CSAS	APC-S

4.2.1.1. **RPS Function**

The RPS initiates a reactor trip to prevent fuel damage during AOOs in conformance with the requirements of GDC 20 of 10 CFR 50, Appendix A. The PPS also provides a reactor trip to assist the ESFAS in limiting fuel damage and the release of significant amounts of radioactivity during accidents.

The RPS initiates a reactor trip for the conditions stated below. Pre-trip alarms are initiated prior to reaching the trip value to provide audible and visual indication of an approach to a trip condition.

- Variable over power (rate limited setpoint)
- High logarithmic power level (fixed setpoint)
- High local power density (LPD) (contact)
- Low departure from nucleate boiling ratio (DNBR) (contact)
- High PZR pressure (fixed setpoint)
- Low PZR pressure (manual reset setpoint)
- High S/G water level (fixed setpoint)
- Low S/G water level (fixed setpoint)

- Low S/G pressure (manual reset setpoint)
- Low reactor coolant flow (high decreasing rate, minimum value) (rate limited setpoint)
- High containment pressure (fixed setpoint)

4.2.1.2. **ESFAS Function**

The ESFAS initiates the operation of ESF components to mitigate the consequences of the postulated accidents. This includes minimizing fuel damage and subsequent release of fission products to the environment.

There is an actuation signal for each ESFAS. Each actuation system is similar except that specific inputs (and bypasses where provided) and the actuated devices can be different.

There is an ESFAS initiation signal associated with each of the following 6 NSSS and 3 BOP ESF functions:

NSSS
- Safety injection actuation signal
- Main steam isolation actuation signal
- Containment spray actuation signal
- Containment isolation actuation signal
- Auxiliary feedwater for S/G 1 actuation signal
- Auxiliary Feedwater for S/G 2 actuation signal

BOP
- Fuel handling area emergency ventilation actuation signal
- Containment purge isolation actuation signal
- Control room emergency ventilation actuation signal

4.2.1.3. **Control Function**

A CEA withdrawal prohibit (CWP) signal is generated when a CPC-CWP signal is input from CPCS or high PZR pressure pre-trip condition is present.

The CWP signal is sent to the DRCS where it blocks CEA withdrawal.

4.2.1.4. **Alarm Function**

The PPS provides status alarms to the QIAS-N and IPS for the following types of conditions:

- Bistable trips
- Bistable pre-trips
- Operating bypasses
- Trip channel bypasses
- Operating bypass permissive
- PPS in test
- PPS trouble
- RPS initiation
- ESFAS initiation

4.2.1.5. **Test Function**

Provision is implemented to permit manual periodic testing of the complete PPS and ESF-CCS with the reactor operating at power or when shutdown. These tests cover the trip actions from sensor input through the reactor trip function and engineered safety features function initiation. The system test does not interfere with the protective function of the system.

4.2.1.6. **Bypass Function**

a. Trip Channel Bypasses

Trip channel bypasses are provided to remove a trip channel from service for purpose of maintenance or testing. Any number of system parameters may be bypassed, but each parameter can be bypassed on only one channel at any given time. A trip channel bypass forces the system to convert to a 2-out-of-3 logic for the bypassed parameter.

b. Operating Bypasses

Operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing. The following operating bypasses are provided:

- High logarithmic power level bypass
- High LPD and low DNBR bypass
- Low PZR pressure bypass
- CPC-CWP bypass

4.2.1.7. **Interlock Function**

a. Trip Channel Bypass Interlock

The administrative procedure for bypassing prevents the operator from bypassing the same parameter in more than one channel.

b. Manual Test Interlock

Manual testing requires the permissive from function enable (FE) keyswitch and the switch is controlled administratively to allow only one channel test function to be operated at any one time.

c. CPCS Test Interlock

The low DNBR and high LPD channel trips are interlocked such that they must be bypassed in the PPS in order to test the CPCS. This ensures that only one CPCS channel is tested at a time.

4.2.1.8. Operator Module Function

An OM is provided for each of the four PPS safety channels. The OMs are located in the MCR SC to provide the operator with such information as trip, pre-trip and bypass status, initiation circuit status, breaker position and phase current status. The manual switches for operating bypass and setpoint reset control are provided on the MCR SC and RSC.

4.2.1.9. ITP Function

The ITP monitors the PPS channel status. It provides the interfaces between the PPS, and interfaces to external systems for status indication and supports the testing function.

4.2.1.10. MTP Function

The MTP is the primary local HSI for the PPS. It is used to monitor status and testing. Also the MTP provides modification function of setpoints and resetting of ESFAS initiation signals when the FE keyswitch is set as enabled status.

The MTP provides the capabilities to perform surveillance and corrective maintenance, initiate tests, and display detailed system diagnostic messages.

The bistable trip channel bypasses, operating bypass and setpoint reset switches are provided on the MTP switch panel. These switches are directly hardwired to bistable processor (BP) DI modules.

4.2.2. Design Features

4.2.2.1. General

The PPS comprises four redundant channels (A, B, C, and D as depicted on Figure 4.2-2, "PPS Basic Block Diagram"), which perform the necessary bistable logic, coincidence logic, initiation logic and associated maintenance/test functions. The system includes four redundant OMs located in the MCR SC. Four redundant channels are provided to satisfy single failure criteria and support plant availability.

The BPs in each PPS channel receive the sensor input directly from field or through the APC-S as shown on Figure 4.2-3. It also receives hardwired discrete and analog signals from the ENFMS and hardwired discrete signals from the CPCS to perform the bistable trip functions.

An RT or ESFAS coincidence signal is generated whenever two out of the four redundant bistable trip conditions are sensed in the local coincidence logic (LCL) processor for a respective trip function.

The PPS produces discrete output signals from each channel including:

- Pre-trip and trip signals used for Reactor Trip initiation, status and alarms
- Pre-trip and trip signals for each engineered safety function, which are used for initiation of the ESF-CCS and engineered safety function status indication

Bistable trip inputs to the LCL processors may be bypassed to perform maintenance and/or testing for instrument channel inputs and a BP to permit continued operation with the

bypassed channel. The trip channel bypass reduces the 2-out-of-4 voting logic to 2-out-of-3 coincidence.

Monitoring, testing and maintenance of the PPS is provided using both the MTP and ITP located in each redundant safety channel.

The PPS design includes the following features:

- A digital microprocessor based design is employed to take advantage of high accuracy and drift free operation.
- Software-based PLC equipment is utilized to the maximum extent possible.
- Standardization of components, to the maximum extent practicable, is used to minimize personnel training and spare parts inventory.
- Fiber optic cables and data communication are used to the maximum extent practical.
- Software is designed, developed, tested and qualified in accordance with the Technical Report for Software Program Manual (SPM) (Reference 4).
- Mitigating provisions are in place to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Non-combustible and heat resistant materials are used wherever practical and temperature alarms are included in the cabinet design.
- The PPS is designed and manufactured to satisfy Quality Class Q requirements and conforms to the applicable Codes and Standards.
- The PPS is qualified to meet Class 1E and Seismic Category I requirements. Class 1E is defined by IEEE Std. 603-1991 and Seismic Category I is defined by RG 1.29.
- Security provisions within the PPS design include:
  - Equipment located within the PPS cabinets is administratively controlled by door key locks to protect against unauthorized access.
  - Provisions are provided by door switches to remotely indicate (via IPS/QIAS-N) that access has occurred to the PPS cabinets.
  - The PPS operating system and application software are protected against unauthorized alterations by a combination of check sums and control of access to software media.
- The PPS is designed for fail safe operation under component failure or loss of electrical power.
  - A single 120 volts alternating current (Vac) power is provided to redundant direct current (DC) power supplies in each PPS channel. A loss of the 120 Vac power feeds to a PPS channel will cause the safety outputs for the channel to become fail safe state.
  - Each PPS LCL RT processor is supervised by the PLC watchdog timer. The watchdog timer outputs are hardwired to a separate PLC rack to ensure appropriate trip signals are generated for the reactor trip function.
- The hardware and software for the PPS meet the single failure criteria outlined in IEEE Std. 603-1991 and IEEE Std. 379 as augmented by RG 1.53.
- The PPS design follows the applicable portions of the human factors engineering (HFE) guidelines. This guide is a compilation of HFE design requirements and is intended to satisfy pertinent regulations and standards. The following identifies some of the HFE design features.
  - OM - The OMs are located in the MCR SC to provide the operator with such information as trip, pre-trip and bypass status, initiation circuit status, breaker position and phase current status.
  - MTP - The MTP is provided in a separate cabinet in each channel for routine maintenance and surveillance testing by plant technicians. It is

located for easy access, uses a display screen selected for optimum viewing with display page hierarchy and navigation. The MTP FPD also replicates all functions that are on the OM.

- ITP - The ITP is shared by the PPS, CPCS, QIAS-P and ESF-CCS. The ITP sends process input values and setpoint values to IPS through QIAS-N to perform cross channel comparison of trip setpoint and process input values. The ITP supports PPS and ESF-CCS maintenance and surveillance testing.
- Internal equipment - Modular equipment (PLC modules and AC/DC power supplies, etc.) is located to provide easy access.
- Field wiring - Adequate space is provided for field cabling termination via multi-pin connectors or to field terminal blocks.
- Equipment Identification - Labeling of major internal components is provided for easy identification of components.
- Protective covers/shields - Measures are provided to protect personnel from hazardous conditions such as inadvertent contact with electrical power supply terminals, rotating fans, etc.

The PPS architecture is designed to minimize potential single failures and to maximize system reliability and availability. This philosophy results in maximum system availability under single random failure conditions.

Each redundant PPS channel comprises two redundant PPS cabinets, each containing a Bistable Process Station and an LCL Process Station. Each bistable process station contains a single PM. Each bistable PM sends its bistable trip status to each redundant LCL process station in the same channel and to other redundant channels' LCL Process Stations via data communication fiber optic SDL. The redundant LCL Process Stations within each channel receive the bistable trip signals and perform the 2-out-of-4 local coincidence logic for each RT and ESFAS function. Each LCL PM drives digital output (DO) module(s) whose outputs are combined to form the selective 2-out-of-4 coincidence initiation logic. The configuration is shown on Figure 4.2-3.

The system, including the processors, is subject to continuous hardware monitoring and annunciation of failures to maximize system availability. A watchdog timer monitors the operability of PMs.

Each PPS channel includes redundancy and diversity. Different PPS analog input parameters are assigned to each analog input module. Each BP processes the bistable logic in the opposite order to that of the other BP. Both bistable PMs have access to independent measurements of all process inputs. The design includes redundant BP cabinets in each channel. The independent configuration of the I/O and communication devices in redundant cabinets is provided.

The selective 2-out-of-4 initiation logic combination of RPS initiation circuit is designed to permit online testing of upstream PLC equipment without causing PPS output RT initiation signals to occur and still permit valid trip signals to propagate through the system. This design provides hot swap capability for a single PLC card/module, without causing an output initiation signal. A design goal is to enhance the system's fault tolerance by accommodating a single PLC module or data communication link failure in the channel without causing a channel trip or component actuation (i.e., RTSS breaker opening or auxiliary feedwater (AFW) pump/valve operation).

The PPS provides alarms to the QIAS-N and IPS to indicate system abnormalities. The PPS provides status alarms to the QIAS-N via the SDN (to the ITP), and SDL (from the ITP to

the QIAS-N). The PPS also provides status alarms to the IPS via the SDN to the MTP and channelized gateways to the DCS network

The two cabinets in each PPS channel are powered by a single 120 Vac vital bus feed. The PPS is configured with redundant internal power supplies in each cabinet. The DC output is auctioneered. This makes the PPS safety system fault tolerant for internal power supply single failures. A single internal power supply failure will not result in interruption of system operation.

4.2.2.2. **Manual Testing Features**

The PPS includes administratively controlled manual tests. These tests provide the means to confirm the PPS is operating correctly. Manual test features are designed not to interfere with the normal operation of the PPS and can be initiated during plant power operation as well as during plant shut down. To accomplish this, a set of overlapping manual tests, initiated from the MTP FPD, are provided to demonstrate proper operation of the PPS safety functions. The tests are performed over channel paths that range from sensor inputs to the RTSS or the input of the ESF-CCS as shown on Figure 4.2-4.

The tests allow for injection of test signals that replace the actual input or calculated signals and provide monitoring points that can be displayed on the MTP FPD. The test injection points are just before the monitoring point used for a previous test (thus providing overlap). They are used to verify operation of the various processors and SDL communication paths.

These tests are performed under administrative control. Activation of these tests requires setup of administrative preconditions and keyswitch interlock prerequisites as described below.

There are three basic levels of testing as follows:

- Bistable logic test
- LCL logic test
- Initiation test

The bistable logic test monitors the integrity of trip path from BP to the input of LCL including SDL.

The LCL logic test confirms the integrity of the trip path in LCL processor.

The initiation test monitors the integrity from LCL processor to the RPS initiation circuit test. Also, the initiation test confirms the integrity from LCL processor to ESF-CCS GC including SDL.

The ITP together with the MTP provides overall PPS system testing as follows:

- Manual sensor test
- Watchdog timer test
- Interlock test
- AI module accuracy test
- DO module operability test
- RTSS test

Trip Channel Bypass

When a signal is bypassed, that signal is not used in the LCL voting logic preventing injected or failed signals from affecting the downstream logic. Setting of a trip parameter channel bypass will result in the LCL voting changing to a 2-out-of-3 logic. A trip channel bypass is

created when both partial bypasses for a trip parameter are set. Channel bypass is activated by a hardwired trip channel bypass switch on the MTP switch panel. Trip channel bypass switches on the MTP switch panel in the MTP/ITP cabinet (MTC) are connected to BP DI module.

Manual Keyswitch Interlock Permissive – Function Enable

There is a manual FE keyswitch on the MTP switch panel. The FE keyswitch is normally in the 'Disable' position. The FE keyswitch must be in the 'Enable' position to inject a test signal. The MTP FPD touch screen controls for PPS testing are 'Disabled' while the FE keyswitch is not in the 'Enable' position. FE switch is connected to BP DI module.

Administrative Restriction – Test Time-out

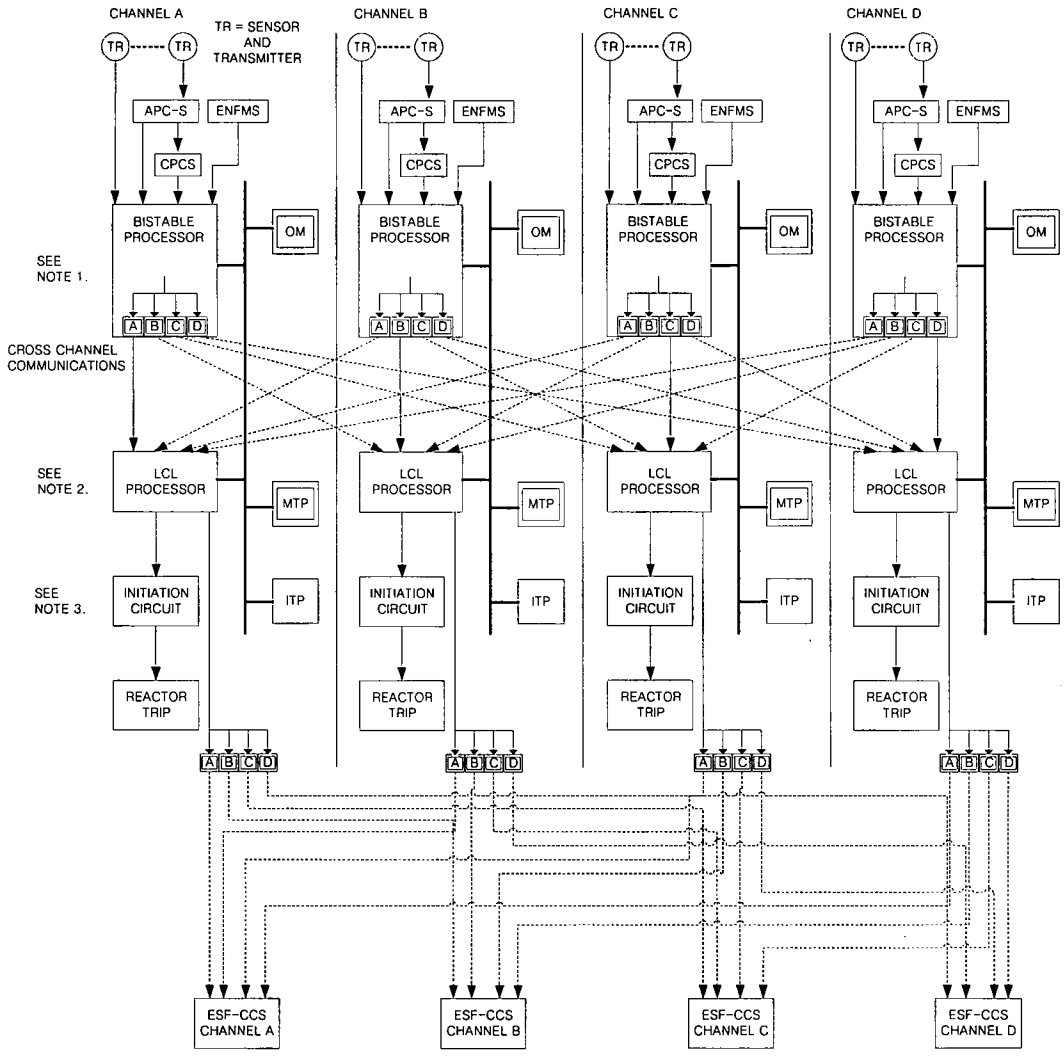
Testing provisions contain a timer that removes the test signals upon time-out. The timer is implemented in the BPs and LCL processors.

4.2.3. Architecture Description

TS

TS

TS



NOTES:
1. ONE TRIP PER PARAMETER SETPOINT. 2 BISTABLE RACKS PER CHANNEL. 1 BISTABLE PROCESSOR PER RACK.
2. 2 LCL RACKS PER CHANNEL.
3. ONE INITIATION CIRCUIT PER CHANNEL FOR REACTOR TRIP FUNCTION.
4. ———— HARDWIRED CABLE
   – – – – – – – – FIBER OPTIC CABLE

Figure 4.2-2 PPS Basic Block Diagram

TS

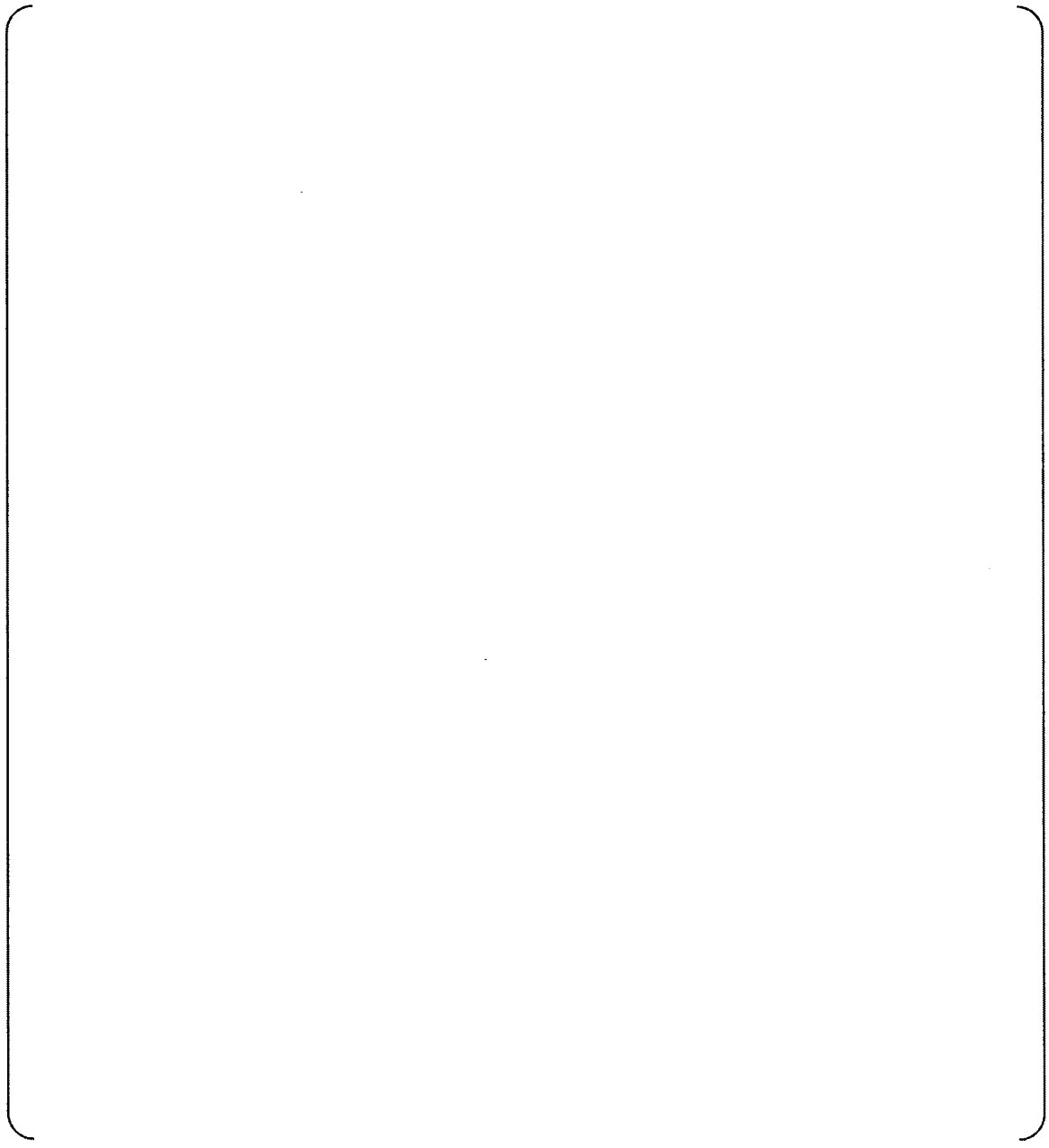


Figure 4.2-3 Typical PPS Channel A Trip Path Diagram

TS

Figure 4.2-4 Overlap in Functional Testing for the PPS

4.2.4. System Interfaces

The PPS cabinet interfaces with the following equipment:

- Auxiliary process cabinet - safety
- Core protection calculator system
- Ex-core neutron flux monitoring system
- Reactor trip switchgear system
- Engineered safety features - component control system
- Information processing system
- Qualified indication and alarm system - PAMI
- Qualified indication and alarm system - non-safety
- Vital bus power supply system
- Control panel multiplexer
- DRCS remote I/O cabinet
- Operator module

The APC-S provides four channels, physically and electrically separate signals for each safety-related plant parameter to the PPS cabinet via hardwired cables.

The CPCS provides four channels, physically and electrically separate DNBR and LPD states to the PPS cabinet via hardwired cables.

The PPS receives the log power, calibrated linear power, log power operating bypass permissive, and ex-core trouble annunciation for the power trip test interlock from the ENFMS safety channel via hardwired cables.

The RTSS interfaces are in the form of relay contacts which are wired to the reactor trip switchgear. The RTSS interrupts power to the DRCS to allow gravity insertion of the CEA's upon receipt of a trip signal which is generated by either the RPS section of the PPS or one of the two sets of manual reactor trip pushbutton on the MCR SC.

The PPS sends the ESFAS initiation signals to the ESF-CCS GCs in the same channel and the other three redundant ESF-CCS channels through CCC SDL.

The PPS sends the digitized value of the monitored plant parameters to the QIAS-P via SDN.

The PPS provides status alarms to the IPS and QIAS-N via MTP and ITP.

Each channel of the PPS is powered from a VBPSS inverter. Each channel of the VBPSS provides a non-interruptible battery backed 120 Vac, single phase, ungrounded power source for essential instrumentation and plant control. The RSR provides the capability to control selected equipment and monitor selected plant variables necessary to achieve an orderly plant hot and cold shutdown when the MCR is uninhabitable.

The conventional switch signals in the MCR and RSR are sent to the PPS by using CPMs and SDL.

The DRCS remote I/O cabinet receives a CWP signal from PPS's D channel only. A CWP logic signal is transmitted to the DRCS when a 2-out-of-4 coincidence condition occurs on either a CPC initiated CWP or PPS high PZR pressure pre-trip signal. This signal is treated as an associated circuit and isolated at the DRCS remote I/O cabinet.

The OM in each channel is shared by the PPS and CPCS. The OMs are located on the MCR SC and provide the PPS status (trip/pre-trip/bypass), initiation circuit status, TCB phase

current status and operating bypass information to the operator. Physical separation and electrical isolation are provided between OMs of redundant channels.

The PPS cabinets are located in channelized I&C equipment rooms. Equipment and circuits of the PPS require four channel separation and mechanical isolation meeting the requirements of IEEE Std. 384 and RG 1.75.

Communications cabling between redundant PPS channels is routed via fiber optic cables. The fiber optic cables satisfy the isolation and independence requirements.

The ESFAS initiation outputs from each PPS channel to the four channel ESF-CCS cabinets are routed and isolated using fiber optic cables.

4.3. Core Protection Calculator System

4.3.1. Functions

The core protection calculator system (CPCS) generates low DNBR and high LPD trip signals. The CPCS monitors pertinent reactor core conditions and calculates DNBR and LPD values from monitored process parameters in each of four redundant core protection calculators (CPCs).

The CPCS provides DNBR and LPD pre-trip and trip signals when either the calculated DNBR or LPD approaches or exceeds its respective setpoint or when certain auxiliary conditions are met. The CPCS channel pre-trip and trip outputs are used by the PPS logic where 2-out-of-4 voting is performed to generate a reactor trip signal.

4.3.1.1. Trip Functions

DNBR Trip

The low DNBR trip is provided to trip the reactor when the calculated DNBR approaches a preset value. The calculation of DNBR is performed by the CPCS based on core average power, reactor coolant pressure, reactor inlet temperature, reactor coolant flow, and the core power distribution. The CPCS calculation includes allowances for sensor and processing time delays and inaccuracies such that a trip is generated by the CPCS before violation of the DNBR safety limit in the limiting coolant channel of the core during incidents of moderate frequency or infrequent incidents.

LPD Trip

The high LPD trip is provided to trip the reactor when the calculated core peak LPD reaches a preset value. The preset value is less than that value which would cause fuel center-line melting. The calculation of LPD is based on the core average power and the core power distribution and includes a compensation to account for the thermal capacity of the fuel. The calculated trip assures a core peak LPD below the safety limit for peak linear heat rate.

Aux. Trip

The CPCS is also designed to meet additional design bases via auxiliary trip functions. These auxiliary trip functions are:

Variable overpower trip provides protection for sudden power increases. The trip signal is generated when the calculated reactor power increases greater than the setpoint. The setpoint is a variable that changes based on the calculated reactor power within pre-defined rate limits. If the reactor power increases rapidly exceeds the rate limited variable setpoint, the trip signal is generated.

Asymmetric S/G transient trip provides protection for instantaneous closure of the main steam isolation valves to a single S/G. The temperature difference of two cold leg temperatures is monitored. If the difference is greater than the pre-defined setpoints, the trip signal is generated.

Range trips on several parameters assure the core conditions are within the analyzed operating space. If the input values or certain calculated variables exceed the pre-defined ranges, the range trip signal will be generated.

Pump trip precludes operation with fewer than two RCPs running. hot leg saturation trip precludes operation with substantial void in the hot leg fluid. The saturation temperature at measured pressure condition is calculated. If the calculated difference between the current hot leg temperature and saturation temperature is less than the pre-defined value, the trip signal is generated.

Hardware fault conditions provide trip signals whenever the CPC is in test mode, in initialization, or when internal fault conditions occur, or fails to meet the timing requirements.

4.3.1.2. **CEA Withdrawal Prohibit**

In addition to the trip signal, the CPCS generates CWP signal for the DRCS when the pretrip conditions or CEA related conditions, such as reactor power cutback or CEA deviation, are reached. The CWP contact is a separate DO from the CPCS channel to inhibit the withdrawal of CEAs. Each channel of the system generates a CWP input to the PPS so as to produce a CWP signal to DRCS. The system provides CWP input in the form of contact output to the PPS. The PPS generates a CWP signal upon simultaneously receiving CWP inputs from two of the four CPCS channels.

4.3.1.3. **Alarm and indication Function**

The CPCS provides status alarms and indication to the QIAS-N and IPS for the following types of conditions:

- Low DNBR trip/pre-trip
- High LPD trip/pre-trip
- CEA withdrawal prohibit signal
- Field sensor input signals
- Trip buffer display
- Snapshot display
- DNBR margin
- LPD margin
- CPCS calculated values
- CPCS trouble
- Processor failure
- CPCS in test

4.3.1.4. **Operator Module Function**

The shared OM is provided to monitor certain inputs and calculated results and status for operator. The OM has a dedicated area of display for alarm conditions. In the OM, the specific activities such as monitoring of values or changing addressable constants are performed.

4.3.1.5. **Maintenance and Test Panel**

The MTP provides such functions as the capability to modify CPCS addressable constants, and provides such information as system parameters, various system status, and test results. The MTP also provides an interface to initiate and support testing. It is located in the MTC

and is shared with other safety systems within the channel. The MTP provides the isolated interface to the non-safety network through SDN.

Manual switches and/or touch panels are used to enable CPCS control functions such as: addressable constant changes, and test initiation, etc.

4.3.1.6. **Interface and Test Processor**

The ITP is located in the same cabinet as the MTP, separate from the CPC and CEA calculator (CEAC) processors and shared with other safety systems in the same channel. The ITP communicates with the CPCS via the SDN. It provides the interfaces between the CPCS and QIAS-N for monitoring of safety-related parameters by the operator.

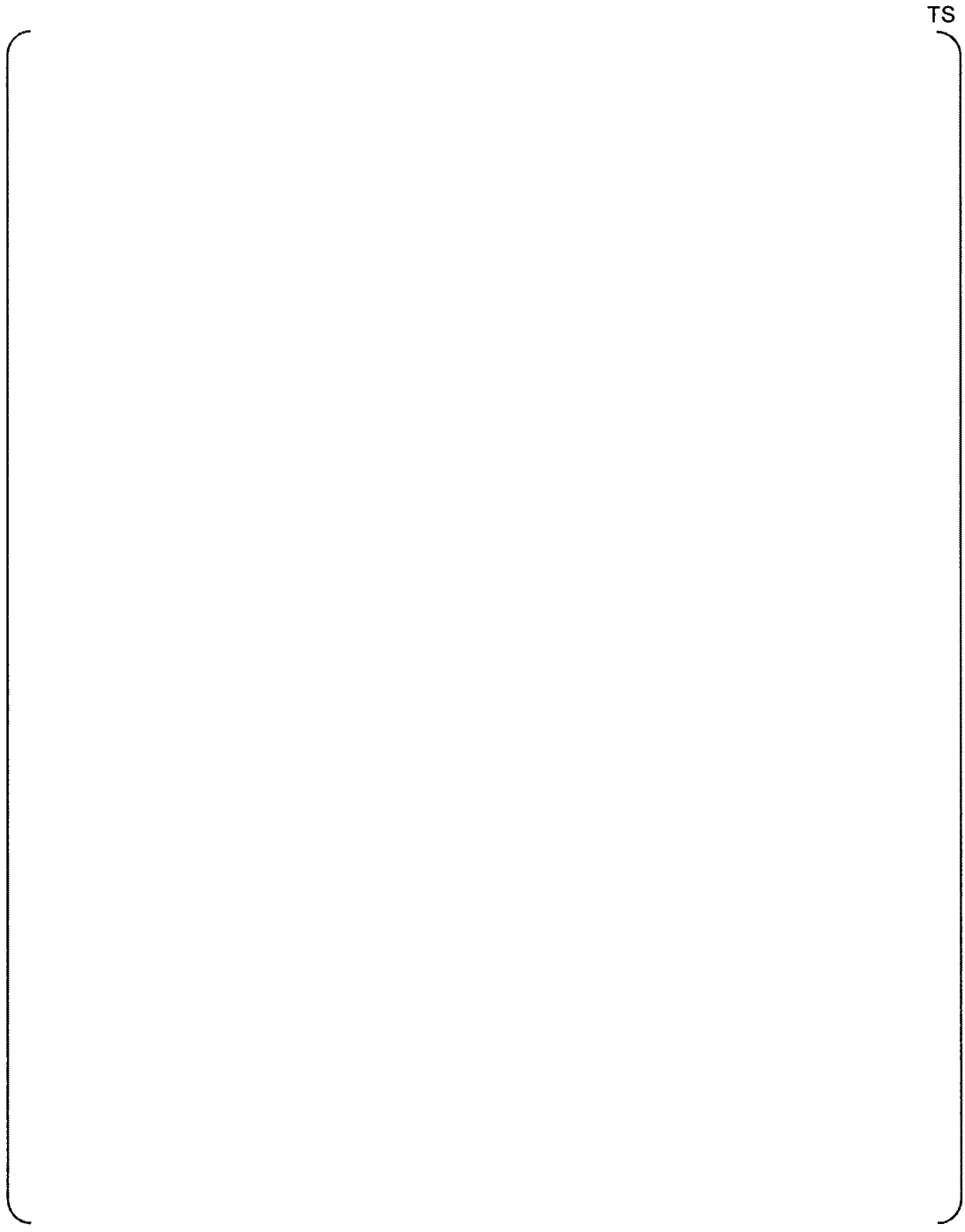


Figure 4.3-1 CPCS Block Diagram

4.3.2. Design Features

4.3.2.1. General

The CPCS consists of four channels of equipment mounted in the four CPCS cabinets and four OMs mounted on the SC in MCR as shown Figure 4.3-1. Each cabinet contains one CPC rack and two redundant CEAC racks. Each channel communicates to OM over SDN. The OM and MTP provide the operator with an interface to the CPCS system and support plant operational activities.

The CPC rack and two CEAC racks utilize the PLCs. The OM and MTP utilize the processor unit with FPD. The PLC rack supports SDL communication and network communication.

Communication between PLCs and OM and MTP is performed using the SDN within the CPCS cabinets, MTC and the OM in the MCR. Communication over a fiber optic cable is used for the network connections between the CPCS cabinets and the OM . The internal network connects all of the PLC stations in each CPCS channel together i.e., CPC Rack, CEAC1 Rack, and CEAC2 Rack, MTP and OM. The network is used to transmit the process data, status and output information to OM and MTP within the safety channel.

SDL communication is used to transmit the safety data within the safety channel or across safety channels. CEA position processor (CPP) 1 and 2 in each CPCS channel redundantly perform an analog to digital conversion on all CEA position inputs to that channel and transmit these CEA positions to the other three CPC channels over fiber optically isolated SDL communication. Each CPCS channel redundantly receives CEA position from the other CPCS channels.

Each CEAC receives analog CEA position measurement signals which originate from one of two reed switch position transmitters (RSPTs) associated with each CEA. Each CEA position is measured by two redundant and independent RSPTs associated with each CEA. There are eight CEACs, two in each CPCS channel. Each CPCS channel has a CEAC 1, using RSPT 1 inputs from all CEAs, and a CEAC 2, using RSPT 2 inputs from all CEAs. RSPT inputs to each CPCS channel shall be converted to digital format in the channel analog input module A/D converter, and transmitted to the other three CPCS channels via optically-isolated SDL.

The CEAC calculates the magnitude of CEA deviation penalty factors (PFs) based upon CEA position sensor input data obtained from each RSPT. After calculating PFs, each CEAC transmits PFs to CPC within CPCS channel via SDL.

4.3.2.2. Design Implementation

CPCS is a digital computer based design to take advantage of high accuracy and drift free operation.

- Utilizes same platform as PPS.
- Multiplexes I/O and data communication to the maximum extent practical.
- Uses software that is designed, developed, tested and qualified in accordance with the SPM.
- Designed to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Non-combustible and heat resistant materials are used wherever practical throughout the CPCS equipment.

Security provisions within the CPCS design include:

- Equipment located within CPCS cabinets is administratively controlled by door key locks to protect against unauthorized access.
- The CPCS software is protected against unauthorized alterations (this includes setpoints and code) by control of access to software media by the plant owner.
- A memory protection key lock in each CPCS channel prevents unauthorized alteration of the software.

TS

TS

TS

4.3-2 CPCS Function Block Diagram

TS

4.3.2.3. **Channel Independence**

4.3.3. Architecture Description

TS

TS

[ ]

4.4. System Interfaces

The CPCS interface with other system is shown in Figure 4.3-3. The CPCS cabinet housing the CPC and CEACs typically interfaces with the following equipment:

- Auxiliary protective cabinet - safety
- Ex-core neutron flux monitoring system
- Reactor coolant pump shaft speed sensing system
- Reed switch position transmitter
- Plant protection system
- Information processing system
- Qualified indication and alarm system - non-safety
- Vital bus power supply system
- Field sensors

4.4.1.1. Auxiliary Process Cabinet-Safety

CPC processor receives the PZR pressure signal from APC-S used for DNBR and LPD calculation.

4.4.1.2. Ex-core Neutron Flux Monitoring System

CPC processor receives the linear sub-channel power signal from ENFMS. These are used to calculate the reactor power calculation and power distribution calculation.

4.4.1.3. Reactor Coolant Pump Shaft Speed Sensing System

CPC processor receives RCP Speed signal from Reactor Coolant Pump Shaft Speed Sensing System (RCPSSSS) for the flow rate calculation.

4.4.1.4. Reed Switch Position Transmitter

CEA position is provided by two RSPT inputs on each CEA. All RSPT inputs are converted to a digital value in CPP and are input to all four CPC/CEAC channels over fiber-optically isolated data links. CPPs in channel A(D) receives 23 CEA positions from RSPT1(2), and CPPs in channel B(C) receives 70 CEA positions from RSPT1(2).

4.4.1.5. Plant Protection System

CPCS system provides the following signals to PPS.

- Low DNBR Trip/Pre-trip

- High LPD Trip/Pre-trip
- CEA Withdrawal Prohibit

4.4.1.6. **Information Processing System**

CPC and auxiliary CPC processor send CPC data to the IPS via the MTP. CEAC also sends CEAC data to the IPS via the MTP.

4.4.1.7. **Qualified Indication and Alarm System-Non safety**

CPCS sends pre-selected data to the QIAS-N via the ITP.

4.4.1.8. **Field Sensors**

CPCS receives the following field sensor signals.

- Hot leg temperature loop 1
- Hot leg temperature loop 2
- Cold leg temperature loop 1
- Cold leg temperature loop 2

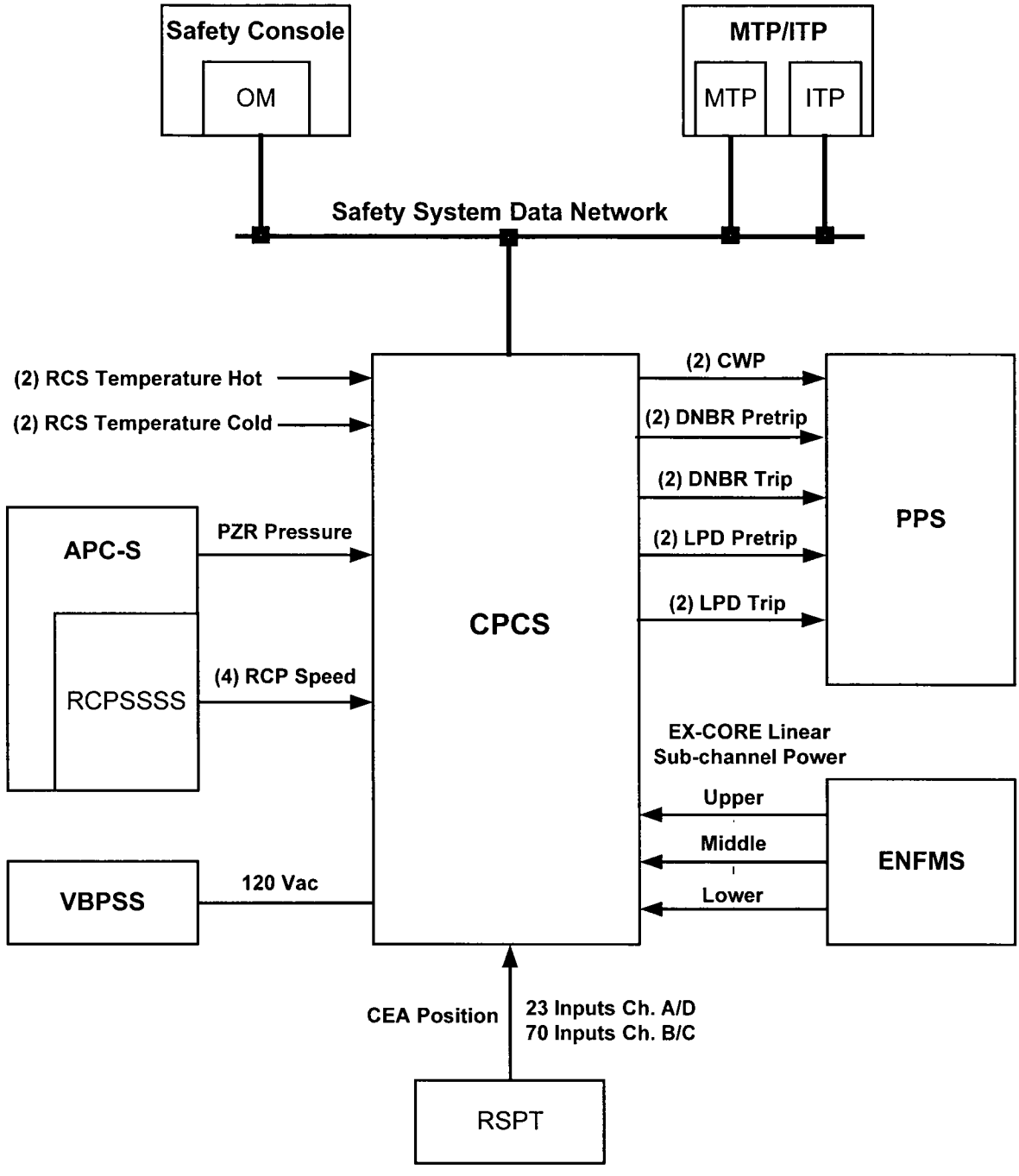


Figure 4.3-1 CPCS Interface Block Diagram

4.5. Engineered Safety Features - Component Control System

4.5.1. Functions

The ESF-CCS consists of the electrical and mechanical devices and circuitry from sensors to actuation device input terminals that are involved in generating those signals which actuate the required ESF systems.

The ESF-CCS serves the functions of actuating ESFAS and executing component control through interfacing the ESFAS portion of PPS as shown Figure 4.4-1. The ESF components receive actuation signals from output of component logic in ESF-CCS, which is functionally interfaced with the PPS, or from the operator. The component control logic provides sequencing necessary to provide proper ESF systems operation. The ESF-CCS LC sends control signals to the ESF components through CIM.

The ESF-CCS provides the control of other safety-related components as well as the actuation of ESF systems component. Such components include breaker and relay operated components (e.g., pumps, fans, heaters and motor operated valves), and solenoid operated components (e.g., pneumatic, electro-pneumatic and direct operated valves).

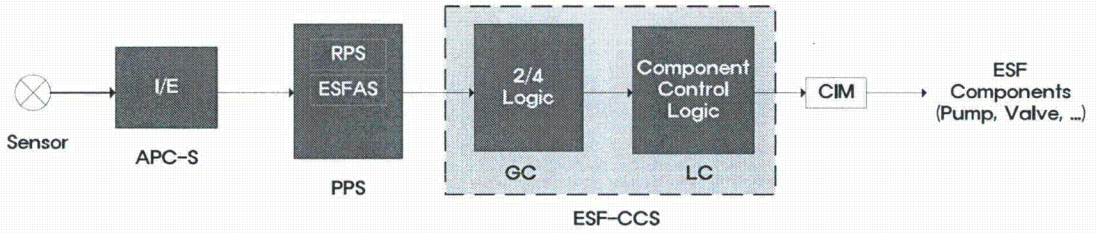


Figure 4.4-1 ESF-CCS Functional Block Diagram

4.5.2. Design Features

The ESF-CCS consists of four independent channels (Channels A, B, C and D) which are electrically and physically independent. The ESF-CCS configuration is based on PLC platform, which are shown in Figure 4.4-2. NSSS ESFAS initiation signals are received from the PPS and BOP ESFAS initiation signals are received from safety-related divisional cabinet (SRDC) of radiation monitoring system (RMS). These signals are transmitted via fiber optic SDL to maintain channel independence.

NSSS ESFAS

Each ESF-CCS channel receives ESFAS initiation signals from all four channels of the PPS and performs an automatic initiation of the affected ESF system(s) when certain coincidence logic conditions are satisfied. The ESF-CCS also provides provisions for manual system level actuation and manual component control of ESF components. The 2-out-of-4 actuation logic is performed in the ESF GC 1 and 2 process stations which independently receive ESFAS initiation signals from four PPS channels (Channels A, B, C and D) and perform a 2-out-of-4 coincidence voting logic on the initiating signals. Valid ESF system level initiation signals are latched and require manual reset for returning to non-actuation status Two redundant GCs (GC 1 and GC 2) are provided for availability within each ESF-CCS channel (Figure 4.4-2). There is an ESF initiation signal associated with each of the following 6 NSSS ESF functions:

- Safety injection
- Main steam isolation
- Containment spray
- Containment isolation
- Auxiliary feedwater for S/G 1 (valve portion of logics does not latch)
- Auxiliary Feedwater for S/G 2 (valve portion of logics does not latch)

Based on the outputs of the coincidence logic, the ESF GCs 1 and 2 provide actuation signals to the associated in-channel LCs via fiber optic SDLs. Each ESF LC receives the ESF actuation signals from the both ESF GCs 1 and 2 and activates the appropriate control action for the associated ESF components.

BOP ESFAS

A redundant set of safety-related instrumentation and controls are provided for proper actuation of the BOP ESFAS equipment to mitigate the consequences of the fuel handling accidents in the reactor containment building and the fuel handling area as well as to provide a habitability condition for the plant operating personnel in the MCR during all phases of the DBE.

The BOP ESFAS consists of safety-related redundant radiation monitoring sensors strategically located in the reactor containment building, fuel handling area, and control room air intake. The following BOP ESF actuation signals are generated by the ESF-CCS when the monitored variables reach the levels that are indicative of a condition which require protective actions:

- Fuel handling area emergency ventilation actuation signal (FHEVAS),
- Containment purge isolation actuation signal (CPIAS)
- Control room emergency ventilation actuation signal (CREVAS)

The LCs provides discrete ESF activation signals to the associated CIM. The CIM mediates the ESF activation signal for the component control between the LC, the DMA switches, and where applicable, the DPS. Any non-discrete components which require modulation are controlled via the analog output (AO) module.

The ESCM provides the operators with primary manual control means for other safety components as well as ESF components. They are located at the operator consoles in the MCR and RSR and SC in the MCR. Accesses to all ESF safety-related components are provided.

In addition, minimum inventory (MI) switches are provided as backup manual control means while the operation by the operator console is unavailable. These switches are located at

the MCR SC. The MI switches provide the MCR operators with manual control means, which are physically independent from the ESCM, for performing emergency operation procedure and plant safe shutdown. The MI is a subset of all safety-related components and includes those components which are associated with assuring a safe reactor shutdown and accident mitigation. The MI switches for component control are directly connected to ESF-CCS LC through control panel multiplexer (CPM), and the system level actuation MI switches are hardwired to ESF-CCS GC.

For each ESF function, there is an associated group of outputs. Each group of outputs is divided into subgroups. Outputs within a subgroup are tested concurrently and are selectively arranged so that concurrent actuation does not adversely affect plant operations.

4.5.3. Architecture Description

TS

4.5.3.1.

TS

TS

Figure 4.4-2 ESF-CCS Configuration

TS

Figure 4.4-3 ESF-CCS Block Diagram

4.5.4. System Interfaces

The ESF-CCS interfaces with the following equipment:

- Plant protection system
- Maintenance & test panel/interface & test processor
- Auxiliary Process Cabinet-Safety
- Control panel multiplexer in the MCR and RSR
- Information processing system
- Qualified indication and alarm system - PAMI
- Qualified indication and alarm system - non-safety
- Vital bus power supply system
- Motor control center
- Component interface module
- Field instrumentation

The PPS ESFAS initiation signals go to the ESF-CCS and form the 2-out-of-4 logic. Fiber optic cables run in conduit provide the isolation and separation between the redundant PPS initiation signals and ESF-CCS channel A, B, C and D equipment.

The BOP ESFAS initiation signals are transmitted from SRDC in RMS to ESF-CCS GC and form the 1-out-of-2 logic. Fiber optic cables are used for the isolation and separation required between the SRDC in RMS and ESF-CCS Channel A and B equipment.

The ESF-CCS GCs and LCs exchange the necessary data with the MTP and ITP through the SDN.

The Manual ESF actuation switches are connected to CPM in the MCR SC and RSR console using hardwired cables. The CPM sends manual ESF actuation signals to ESF-CCS via fiber optic SDL.

The ESF-CCS inputs to QIAS-P from the same channel shall be provided via SDN and from other channel via ITP.

The ESF-CCS provides its operating status information including ESFAS actuation status, cabinet trouble alarm and system in test to IPS and QIAS-N through MTP and ITP respectively.

Each channel of the ESF-CCS is powered from Class 1E inverters in the each channel of the VBPSS which provides a reliable, continuous 120 Vac, single phase, ungrounded power for essential instrumentation and plant control.

The ESF-CCS receives the component control signals from ESCM through SDN and MI signals through SDL via CPM.

The ESF-CCS provides discrete ESF actuation signals to the associated CIMs.

Each ESF-CCS channel is located in a different fire zone, which contains a minimum of combustible materials. The ESF-CCS LC cabinets are located near controlled plant components.

Equipment and interfacing circuits of each ESF-CCS require four channel separation and mechanical isolation meeting the requirements of IEEE Std. 384 and RG 1.75.

4.6. Qualified Indication and Alarm System – PAMI

4.6.1. Functions

The function of the QIAS-P is to provide a continuous display of AMI variables (Types A, B and C) and an unambiguous indication of the approach to and the recovery from ICC.

The QIAS-P calculates core exit temperature from the core exit thermocouples (CETs). The QIAS-P calculates primary coolant saturation margins based on CET temperatures, hot and cold leg temperatures, heated junction thermocouple (HJTC) temperatures from the reactor vessel head region, and PZR pressure. The QIAS-P calculates reactor vessel coolant water level based on the signals from the HJTCs.

The QIAS-P provides output signals for QIAS-P display and the IPS via MTP, and for QIAS-N via ITP and data link, after communicating through the SDN. The output signals are for display of sensor signals, ICC variables and/or AMI variables.

The QIAS-P provides a backup for the safety parameter display system (SPDS) for ICC variables. The SPDS function is implemented in the safety parameter display and evaluation system+ (SPADES+) within the IPS.

Upon receipt of the analog and digital signals, QIAS-P performs signal checking such as range check. The alarms and displays provided by QIAS-P are a major part of the overall MCR information system used for normal plant operation and accident monitoring. Overall system configuration is presented in Figure 4.5-1.

4.6.2. Design Features

The QIAS-P has two channelized cabinets. The QIAS-P cabinet for each channel is geographically distributed into channelized I&C equipment room. The QIAS-P receives AMI variables from the PPS and ESF-CCS via network connection and, APC-S and process instrumentation via hard-wired connection.

4.6.2.1. Calculation

The QIAS-P processes the AMI variables (Types A, B and C) determined based on RG 1.97, Rev.4 for accident monitoring.

The QIAS-P calculates a representative CET temperature from the CETs. The QIAS-P calculates reactor coolant saturation margin based on hot leg and cold leg temperatures, PZR pressure, and core exit temperatures, and unheated thermocouple temperatures. The QIAS-P also calculates the reactor vessel water level and the HJTC heater power output based on the HJTC signals.

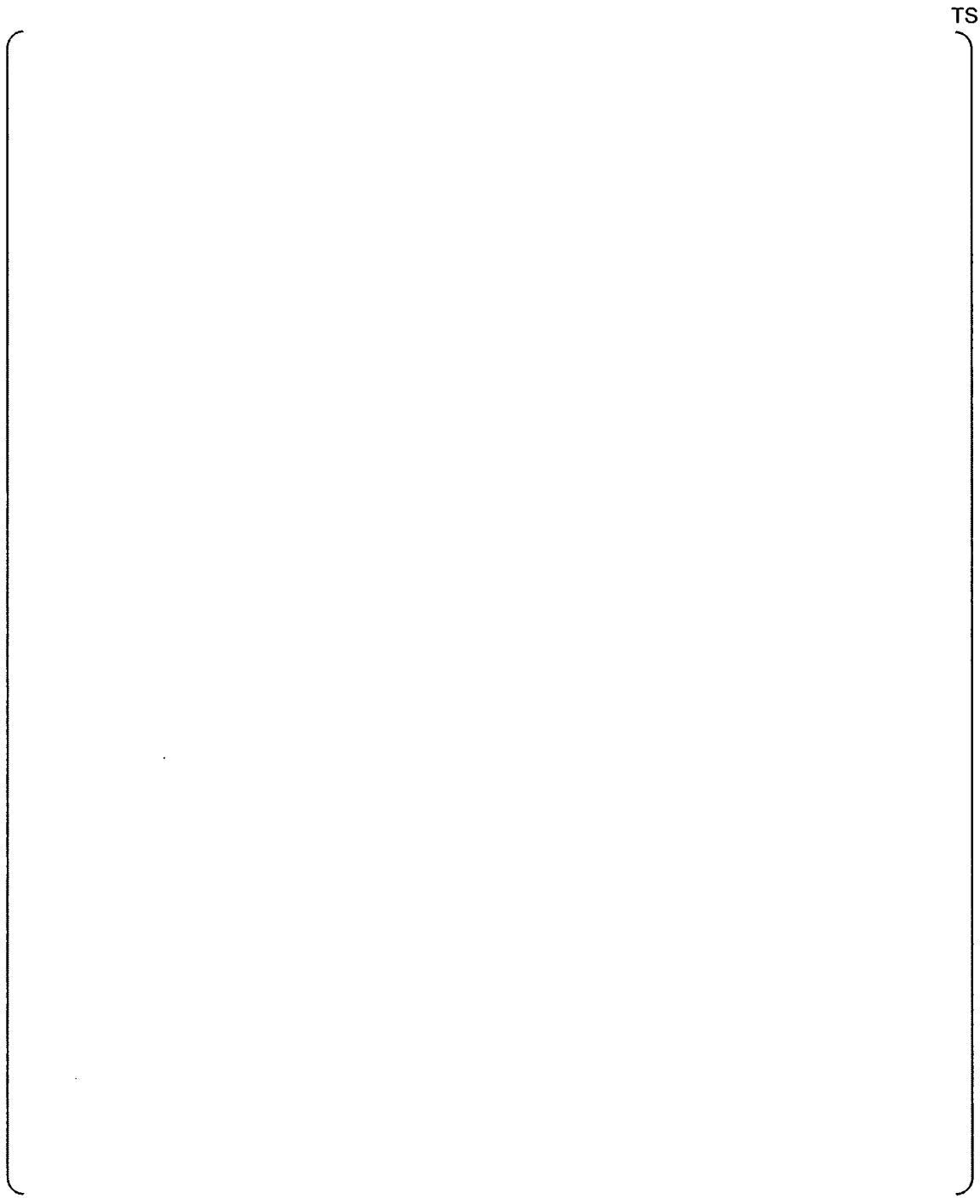


Figure 4.5-1 QIAS-P Block Diagram

4.6.2.2. **Displays**

The QIAS-P drives two FPDs which are mounted on the SC located in the MCR. The QIAS-P channel A(B) displays channel A(B) variables only For CIVs, the QIAS-P A(B) displays the valve status for all channels.

The QIAS-P FPD displays AMI variables (Types A, B and C) determined based on RG 1.97, and also provides backup displays for the ICC variables per NUREG-0737. The primary displays are implemented in the SPADES+.

The FPDs are configured with a device to allow the operator to interface with the QIAS-P. Each FPD allows the operator to select display pages that output either:

- AMI variables or
- ICC variables

The FPDs output an unambiguous indication in accordance with HFE convention. The following ICC variables are calculated and validated by the QIAS-P processing controller, and are displayed on the QIAS-P displays in the MCR.

- Primary coolant saturation margin (temperatures calculated from RTDs, HJTCs, CETs and PZR pressure)
- Coolant temperature at the core exit (calculated from CETs)
- Coolant level in the reactor vessel (calculated from HJTCs)

4.6.2.3. **MTP Functions**

The QIAS-P allows signal substitution, signal bypass, and setpoint changes by operator through MTP to prevent software modifications for simple changes to the system. These functions are manually initiated from the MTP.

4.6.2.4. **Power Supply**

Power distribution to each channel is assigned such that the loss of a single vital instrument power bus will not result in the loss of more than one set of QIAS-P controller processor and QIAS-P display. Loss of electrical power to a QIAS-P display results in a blank screen. Loss of electrical power to one QIAS-P controller processor results in an indication of an inactive state on the QIAS-P displays.

4.6.2.5. **Alarms**

The QIAS-P generates the alarm (visual only) for parameters of ICC.

4.6.2.6. **Redundancy**

The QIAS-P consists of the redundant safety channels A and B for signal processing and displays. Redundancy is provided for both the instrument channels supplying the signal and the displays in the MCR. Instrument channels are electrically isolated and physically separated from non-safety equipment by qualified isolation devices. The cabinets are located in separated I&C equipment rooms. Credited redundancy for the display of Type A/B/C variables is provided by the QIAS-P and the variables are also presented on the QIAS-N and IPS. The IPS is physically separated and independent from the QIAS-P.

To prevent ambiguity of the information presented to the operator the information system employs a number of features to ensure that the information presented to the operator is correct.

The QIAS-P monitors two redundant AMI instrument channels A and B for each Type B and C process parameters. For CIVs, the QIAS-P displays all channels within one channel. Type A variables are displayed using conventional indicator on the SC.

Channels A and B are displayed to allow the operator to select the correct instrument based on his evaluation of data from the QIAS-N, the IPS and/or other related process measurements.

4.6.3. System Interfaces

The QIAS-P cabinet interfaces with the following systems and equipment:

- Process instrumentation
- Auxiliary process cabinets - safety
- HJTC (HJTC temperatures)
- ICIS (CET temperatures)
- DIS
- ESF-CCS
- PPS
- MTP (then to IPS),
- ITP (then to QIAS-N),
- QIAS-P display

The HJTC heater power signals to HJTCs go directly via a hardwired cable.

The Table 4.5-1 shows a summary of the I/O signals for the QIAS-P.

TS

Table 4.5-1 Summary of I/O Signals for QIAS-P

4.7. Data Communication System

The data communication systems (DCSs) provide high speed and error free communication path between each segment within intra-channel or between control/protection systems and information systems or within the information systems. The DCSs are designed to ensure that any errors in data communication do not trigger incorrect function or prevent the safety functions from being performed through the design with accurate, reliable and timely transmission.

4.7.1. Design Features

4.7.1.1. Safety and Quality Classification of Components and Modules

The fiber optic modems, communication cables and communication modules used in DCS of the safety I&C systems are classified into Class 1E, Quality Class Q and Seismic Category I.

4.7.1.2. DCS Software Quality

The DCS is classified as follows in accordance with the SPM.

- Cross channel communication SDLs – protection
- ESF-CCS GC to LC SDLs – protection
- CPM to ESF-CCS SDLs - protection
- Safety system data network (SDN) – important to safety
- ITP network – important to safety
- ITP to QIAS-N network – important to safety
- MTP to IPS network – important to safety

4.7.1.3. Performance (Real time & Deterministic timing)

The DCS application software is deterministic (repetitive and non-interrupt driven). Deterministic means that the function of the application program is predictable and reproducible. The execution sequence of an application is not influenced by internal decision logic or external interruption. The execution sequence of an application program is repeated at predetermined intervals.

The DCS time delay is considered in establishing the instrument setpoints.

Because of the deterministic operation of the communication design, there will be no difference in data transfer rate, data bandwidth, data accuracy and error performance during normal and abnormal operations.

4.7.1.4. Reliability

Error checking technique is incorporated into the communication protocol to assure the integrity of the transmitted data.

Upon detection of the communication loss within a safety system, the system is designed that communication failures shall not prevent safety systems from performing their

intended safety function. The FMEA considers the credible failures of all components including communication modules and communication links/networks.

The reliability of application level communication software is assured by implementing the SPM.

4.7.1.5. **Control of Access**

Security provisions (access control) are provided for the DCS same as the connected system.

4.7.1.6. **Single-Failure Criterion**

The DCS is designed with redundancy and multiple data paths where essential data communications are necessary. The FMEA to be performed for the safety I&C systems describes and provides a detailed evaluation; including network cable and equipment failures, failure to transmit and receive data or transmission of erroneous data.

The DCS is designed so that the requirements of the single failure criteria (SFC) are satisfied. The FMEA shows that no single failure will defeat more than one of the four redundant safety I&C systems channels as applicable.

4.7.1.7. **Independence**

The DCS is designed to maintain the independence between the safety channels (A, B, C, D), and the independence between the safety and non-safety systems.

Communication between safety I&C systems are performed via fiber optic cables only.

The communication independence is designed to satisfy ISG-04.

4.7.1.8. **Failure Modes (including Fail-Safe Design Strategy)**

The safety I&C systems including DCSs are designed to fail into a safe state or into a state established as acceptable in the event of loss of power supply. These systems are also designed so that any single failure will not prevent proper protective action at the system level. The FMEA shows that no single failure will defeat more than one of the four redundant channels of safety I&C system and prevent proper protective action at the system level. The FMEA includes a data communication interface failure to transmit, receive or transmit erroneous data.

With regard to power supply requirements, the PPS function is designed such that the failure of the DCS power supply required for performing the PPS function will result in a reactor trip for that redundant protective channel (fail-safe design). The ESFAS functions of the DCS are designed to ensure that failure of a DCS power supply required to perform ESFAS functions will result in a failure of the related actuation channel as-is (fail-as-is design).

4.7.1.9. **System Testing and Inoperable Surveillance**

System testing and inoperable surveillance for communication are designed as part of the overall design of the safety I&C systems.

The bypassed and inoperable indications for DCSs are consistent with those of the systems of which they belong.

4.7.1.10. EMI/RFI Susceptibility

EMI qualification test on the DCS will be performed as required on each related system.

The data communication media do not provide a fault propagation path due to environmental effects, such as high-energy electrical faults or lightning, from one redundant portion of a system to another or from a non-safety system to a safety system.

4.7.1.11. Diversity and Defense-in-Depth

The D3 analyses address the capability of the overall plant design to cope with the plant design basis event concurrent with a postulated CCF of the entire safety I&C systems including the associated DCS.

4.7.1.12. DCS exposed to Seismic Hazard

The DCS for safety I&C systems is designed and qualified to meet Seismic Category I requirements.

4.7.2. System Description

As shown in Figure 4.6-1, the PPS and ESF-CCS data communication network consists of SDN, CCC-SDLs, ITP network, PPS to ESF-CCS SDLs, CPM to PPS/ESF-CCS SDLs, MTP to IPS interface and ITP to QIAS-N interface.

TS

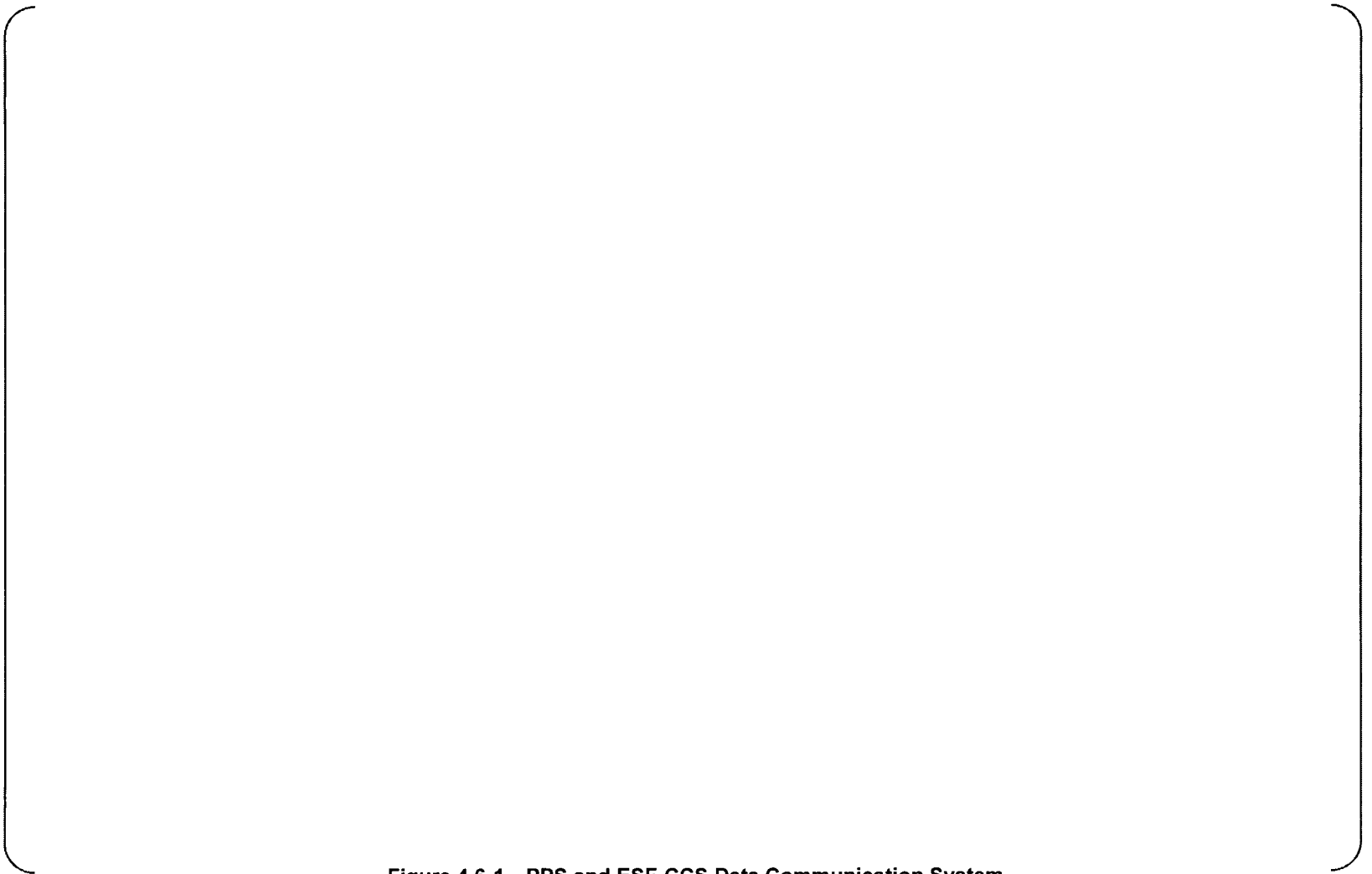


Figure 4.6-1 PPS and ESF-CCS Data Communication System

4.7.2.1. Cross Channel Communication Serial Data Links

There are two sets of CCC SDLs per redundant PPS channel. These SDLs originate in the bistable PMs.

Each PM is composed of two sections each having their own processor. One side is called the processing section (PS) and this section executes the safety-related application program. The other section is called the communication section (CS) and this section is the interface for the SDL. Each CS in the PM supports SDL communication. Each bistable PM broadcasts data to the LCL processors connected to its SDL. The SDLs connected to redundant PPS channel LCL PMs use fiber optic modems and cable to provide independence and isolation. CCC SDLs are also used to transmit ESF actuation signals from the LCL PMs to the ESF-CCS GCs in the same channel and to the three redundant ESF-CCS channels using fiber optic modems.

The fiber optic communication used for the CCC SDL between the redundant PPS channels is RS-422 serial data transmission link. The CCC SDL's purpose is to provide the bistable trip information to the LCL PMs and send ESFAS initiation signals from LCLs to ESF-CCS GCs in all channels.

Failure of a bistable PM is compensated by the redundant BP in the channel and not affects LCL. Failure of both BPs in a channel causes LCL to set that channels input signals to a trip state for RPS function and to a no trip state for ESFAS function.

Failure of a LCL PM is compensated by LCL processor in redundant rack in the PPS channel.

To ensure communication independence, each of the bistable and LCL PMs includes two separate processors (one for the processing section and one for the communication section) as shown in Figure 4.6-2. Data flow between redundant PPS channels is buffered at both ends ensuring independence of the redundant channels. One way communication is used for communication isolation and the fiber optic cables are used for electrical isolation. This communication method is also applied to the data link between PPS and ESF-CCS.

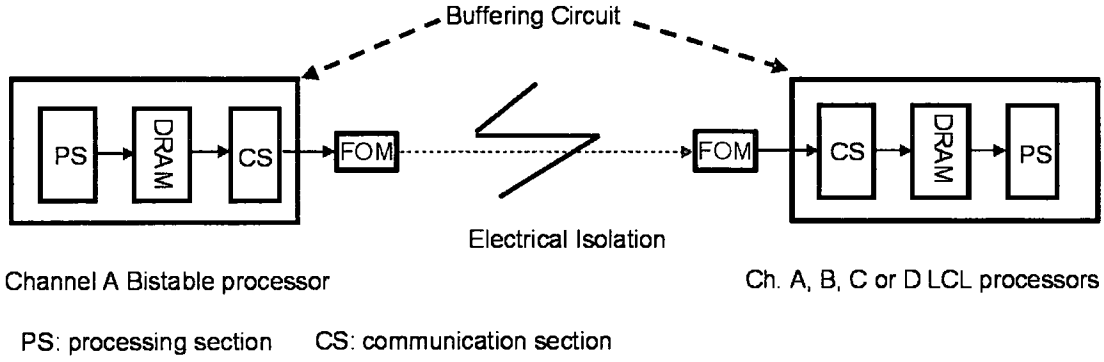


Figure 4.6-2 Data Communication between Redundant Channels in PPS and ESF-CCS

4.7.2.2. Intra Channel Communication Safety System Data Network

The intra-channel SDN connects the PLC stations in each safety channel together (i.e., bistable, LCL, ESF-CCS GC, LC, MTP, ITP, CPCS, etc). This network originates from an independent CI card to form a SDN within a channel.

It allows status and testing information to be provided from each station. The MTP and OM are connected to the SDN for the purpose of status monitoring, setpoint changes, and testing. Failure of this network does not prevent the operation of the safety channel from performing its intended safety function because the SDN is separated from the SDL for control purpose. The network has no interconnection to any of the other three redundant safety channels and therefore is independent

The SDN provides data communication among the following systems and components within same channel:

- PPS bistable processors
- PPS LCL processors
- ESF-CCS group controllers
- ESF-CCS loop controllers
- ESF-CCS soft control module
- CPCS processors
- QIAS-P processors
- Operator module
- Maintenance and test panel
- Interface and test processor
- Control panel multiplexers
- ESCM

4.7.2.3. ITP Network

The ITP communicates with the ITPs in the other safety channels via dedicated SDLs. These SDLs between ITPs are isolated from the SDN in each channel.

The ITP network uses the two way communication using separate receiving line from sending line as shown in Figure 4.6-3.

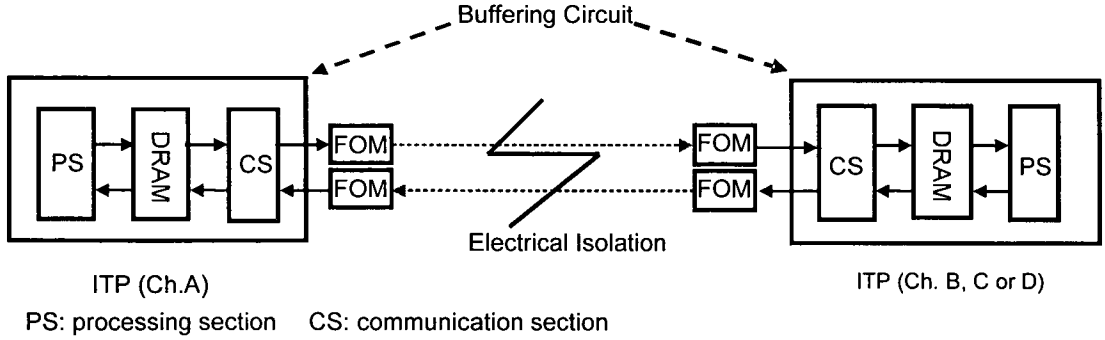


Figure 4.6-3 Interface & Test Processor Network

The ITP to QIAS-N network provides communications between ITPs and QIAS-N. The information for monitoring and/or testing of the safety system and the necessary data are provided to the QIAS-N via the ITP, which performs gateway function. The data flow from the ITP to the QIAS-N is unidirectional. The QIAS-N is programmed only to receive data and the transmission of any un-programmed data is not allowed via ITP. A complete failure of this network will not prevent the safety systems from performing their intended safety functions.

The data flow from safety system to non-safety system is unidirectional as shown in Figure 4.6-4.

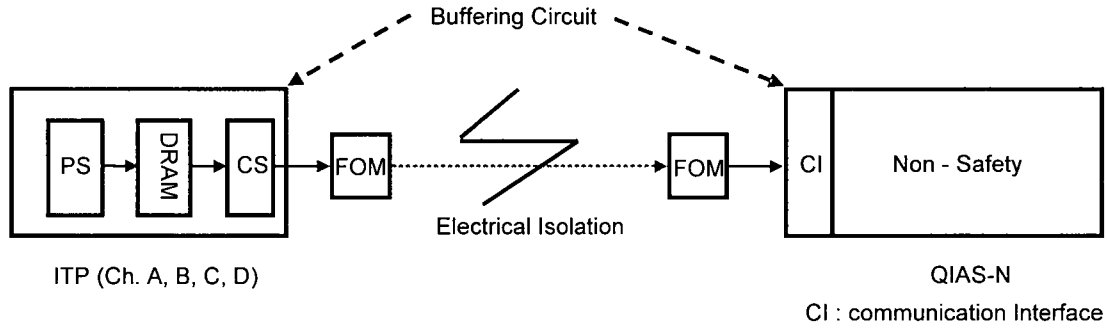


Figure 4.6-4 Data Communication from ITP to QIAS-N

4.7.2.5. **MTP to IPS Network**

The MTP to IPS network is used to provide data transmission to the IPS as shown in Figure 4.6-5. The data flow from the MTP to the IPS is unidirectional via a simplex fiber optic cable.

The communication between the MTP and IPS need not any acknowledgment. A failure of this network will not prevent the RPS and ESFAS functions.

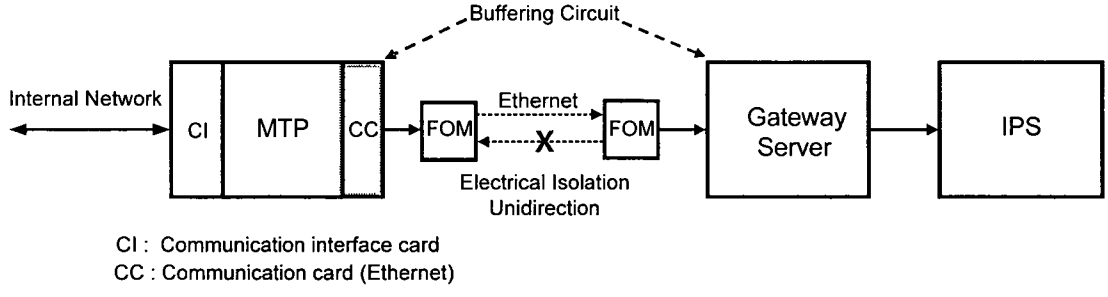


Figure 4.6-5 Data Communication from MTP to IPS

4.7.2.6. **Communication of ESCM**

Data link is used for communication between IFPD to ESCM to send identification data of component. It is unidirectional communication from IFPD to ESCM. A complete failure of this data link will not prevent the safety systems from performing their intended safety functions because the identification data is only used to call up the soft control template on the ESCM FPD.

The data communication between ESCM and the individual safety channels of ESF-CCS is designed with SDN which provides a fault-tolerant and deterministic characteristic. And the corresponding network provides a deterministic function which provides predictable control response. It also provides electrical isolation between each segment. The SDN provides the communication path of the component feedback data from ESF-CCS to ESCM as well as the control signal from ESCM to the ESF-CCS.

Soft control network is shown on Figure 4.7-1.

4.8. Safety HSI System

4.8.1. Safety Control HSI

4.8.1.1. ESF-CCS Soft Control Module

The ESCM provides manual control means of discrete control and modulation control of safety-related plant components which are controlled by the ESF-CCS. The ESCM allows a standard interface template to assume the role of numerous control switches and analog control devices via software configuration. The ESCM is used to provide manual control means as follows:

- Manual actions to provide the component level control capability during plant normal operation
- Manual actions necessary to maintain safe conditions and to bring the plant to a safe shutdown condition during/after DBE

The ESCM is implemented on qualified touch screen-based FPD. Each operator console in the MCR includes four channelized ESCMs. These are communicated with an IFPD directly and a corresponding IFPD is used to call up a template on the ESCM by selecting a symbol of control component on the system mimic display.

The ESCMs are also provided on the SC to support the operation tasks of the pre-designated operator in post-trip conditions as means for controlling related equipment.

Figure 4.7-1 shows a simplified ESF control block diagram.

4.8.1.2. Minimum Inventory Control

The MI controls are used to accomplish plant safe shutdown when all of the operator consoles become unavailable. The MI controls are specified as those controls for:

- Preferred/credited success path components in the major flow path of EOPs
- Components required to perform safe shutdown
- Components required to perform critical tasks identified by the probabilistic risk analysis (PRA)/ human reliability analysis (HRA)

The MI controls are implemented by hardwired switches on the SC. The MI controls of component level are connected to the ESF-CCS controllers through the CPM to simplify cabling and wiring from the MCR to ESF-CCS cabinets.

Manual reactor trip switches are provided for the operator to manually trip the reactor, and the signal from this switch deenergizes the CEDM coils, allowing all the CEA to drop into the core.

Two sets of reactor trip pushbutton are provided on the MCR Safety Consol and one set on the RSC.

The manual ESF system level actuation switches are provided as input signals to execute ESF system actuation. These switches are provided at the SC for manual ESF system level actuation.

4.8.1.3. Safety Console HSI

Safety-related dedicated controls and qualified displays are provided on the SC for manual actuation of the safety systems. Hence, even though all the operator consoles are all failed, the MCR operators can mitigate the accident and maintain the plant in safe condition through the SC. The SC contains the following equipment:

- MI switches for control that are necessary for preferred/credited success path to perform EOP, safe shutdown, and critical tasks identified by PRA/HRA
- QIAS-P and QIAS-N to support manual operator actions for safety function
- DMA switches and DIS to perform plant safe shutdown and critical safety functions when a CCF of safety I&C systems is taken place
- ESCM to provide safety control means not assigned to minimum inventories
- Turbine back-up FPDs, PPS/CPCS OMs, mini LDP to support plant safe shutdown

4.8.2. Qualified Indication and Alarm HSI

The design description of the QIAS-P and QIAS-N are described in Sections 4.1.1.4 and 4.1.2.5, respectively.

4.8.3. Diverse HSI

The diverse HSI provides protections against CCF of all the safety I&C systems which are implemented by the common digital safety I&C system platform. The diverse HSI consists of the DMA switches for control and the DIS for indication. The diverse HSI is used to place the plant in a hot-shutdown condition. In addition, the DMA switches are intended to control critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity. They are provided for system level actuation of main flow path components in the safety system as follows:

- Safety injection (2 trains)
- Containment spray (2 trains)
- Auxiliary feedwater (each SG)
- Main steam isolation (each SG)
- Containment isolation / Letdown isolation (1 train)

The DMA switches are directly connected to fanout devices in the MCR SC to distribute the system level switch signals to the CIM for the applicable ESF components. Details of diversity HSI are described in Sections 4.1.3.2 and 4.1.3.3.

4.8.4. Remote Shutdown Console HSI

The RSR is provided for hot and cold shutdown of the plant outside the MCR. The RSC is a sit-down operator console in the RSR with the same console profile as the MCR operator consoles.

The RSC HSI consists of the following HSI devices:

- Four identical operator consoles
- Four ESCMs
- Shutdown overview display panel
- Two dedicated pushbuttons for two divisions (A, C) of ESF system level actuation switch (MSIS)
- Six dedicated switches for six divisions (A, B, C, D, N1 and N2) of the MCR/RSR transfer switches
- Reactor trip pushbuttons

The shutdown overview display panel (SODP) on the RSC provides the information that the operator requires for quick assessment of the overall plant status.

The MCR and RSR are placed in the physically separated locations equipped with separated ventilation systems, on separated elevations. The displays and controls on the RSC are physically separated and electrically isolated from those of the operator console and SC in the MCR. No single credible events that cause evacuation of the MCR (and/or fire damage in the operator console and SC) cause the RCS to be inoperable.

TS

Figure 4.7-1 Simplified ESF Control Block Diagram

4.9. Reactor Trip Switchgear System

4.9.1. Functions

The RPS signals from PPS are connected to the RTSS which connects or interrupts the power to the DRCS. As shown in Figure 4.8-1, the initiation relays interface with the undervoltage devices in the circuit breakers of the RTSS. Also, the RTSS receives the shunt trip signals from the DPS through the shunt trip devices in the circuit breakers for diverse reactor trip function.

4.9.2. Design Features

Eight RTSGs are connected with 2/4 configuration as shown on Figure 4.8-1. Full 2/4 RTSG configuration with eight RTSGs meets SFC during maintenance and testing.

The PPS provides the under voltage trip signals and the DPS provides the shunt trip signals to each RTSG for diversity.

Two pairs of manual trip switches are provided in the MCR and one pair of manual trip switches is provided in the RSR for reactor trip.

TS

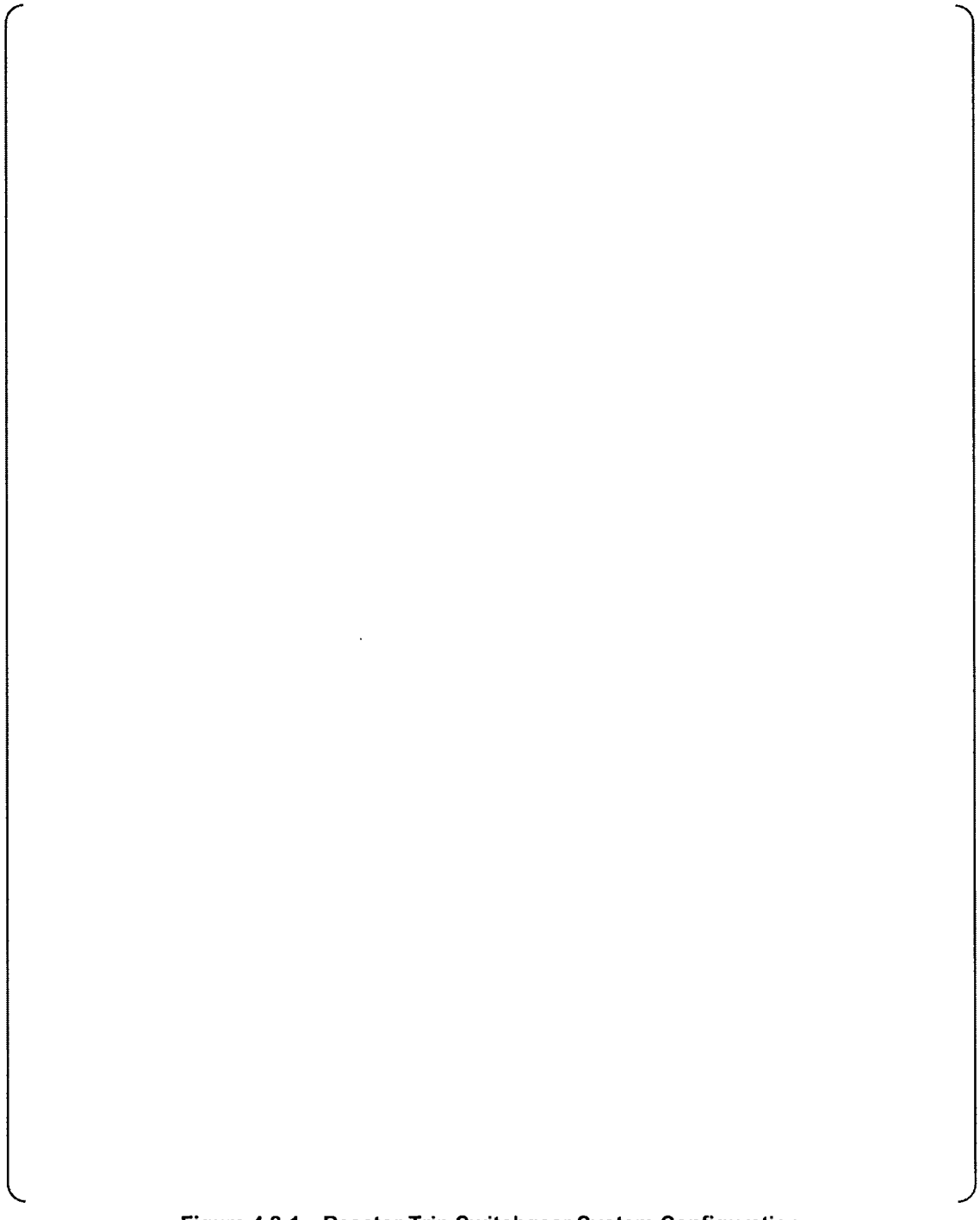


Figure 4.8-1 Reactor Trip Switchgear System Configuration

5. SOFTWARE RELIABILITY

5.1. Software Design Overview

Reliable computer software is essential to the design and operation of the safety I&C systems equipment. The SPM (Reference 4) describes the processes which ensure the reliability and design quality of the safety I&C system and expands the procedural requirements of the Quality Assurance Manual (QAM).

The SPM is based on a software life cycle model consistent with industry standards (IEEE Std.1012 and IEEE Std. 1028 endorsed by RG 1.168) that include the following phases:

- Concept phase
- Requirements phase
- Design phase
- Implementation phase
- Test phase
- Installation and check out phase
- Operations and maintenance phase

The SPM describes the following basic planning elements and provides guidance for generating the required implementation documentation.

a. Software management plan (SMP)

The SMP is the basic governing document for the entire development effort. Project oversight, control, reporting, review, and assessment are all carried out within the scope of the software management plan.

b. Software quality assurance plan (SQAP)

The SQAP describes the process and practice of developing and using software. The SQAP addresses software classification, software categories, software development process, security, software management, documentation, standards, practices and conventions, review requirements, problem reporting, and other software quality issues.

c. Software verification and validation plan (SVVP)

The SVVP describes requirements for the V&V process to be applied to systems. The SVVP addresses overview of V&V, V&V principles, V&V process, V&V testing strategy and V&V activities.

d. Software configuration management plan (SCMP)

The SCMP describes the methodology used in managing the configuration control of software for the systems.

e. Software development plan (SDP)

The SDP provides necessary information on the technical aspects of systems that are required by the software design team in order to carry out the project.

f. Software integration plan (SintP)

The SintP describes integration of software elements, the hardware/software integration process, and testing the result of the integrated product.

g. Software installation plan (SInstP)

The SInstP describes the process for installing the software product to the target hardware.

h. Software training plan (STrngP)

The STrngP describes the process that will be used to train the operators of the software system.

i. Software operations and maintenance plan (SOMP)

The SOMP specifies the requirements for the operation and maintenance of computer software utilized for the systems after delivery.

j. Software safety plan (SSP)

The SSP describes the procedures and measures to maintain and improve the safety of the software system.

k. Software test plan (STP)

The STP describes the process and measures to test intermediate, integrated, and/or final software products.

The compliance to secure development and operational environment (SDOE) guidance for the safety I&C systems in accordance with RG 1.152 is described in the SPM (Reference 4).

The SPM applies to all the software and firmware for the APR1400 I&C system, whether developed in-house, licensed or procured from a commercial vendor, or otherwise acquired for delivery. The acceptance of pre-developed software is based upon the requirements of RG 1.152, IEEE Std. 7-4.3.2 and guidance of EPRI Report TR-106439 .

5.2. Software Classification

TS

[:]

TS

Table 5.2-1 lists the safety class and software class for the safety I&C systems and the associated data communication networks. Specific parts of the software in a system may be assigned to different classes. But all software within a processor is of the same class.

Table 5.2-1 Hardware and Software Classification TS

5.3. Quality Assurance

A SQAP is included in the SPM and will be followed during the development, acquisition, use and maintenance of the safety I&C systems software. Each software quality assurance task is outlined in the SQAP. The plan addresses documentation needed for each of the software life cycle phases identified in Section 5.1.

The types of documents produced in the process of implementing the SQAP are:

- Test plans, cases, procedures and reports
- Review and audit results
- Problem/test exception reports and software change requests
- Software configuration management plans
- Software verification and validation plans

Typical tasks and responsibilities performed during the various software life cycle phases are listed in Table 5.3-1. All documents listed are designated as lifetime quality records in accordance with the requirements of the QAM.

The software development process ensures standardization, compatibility and maintainability of the resulting software products. The software reviews required by the SQAP are technical and designed to verify the technical adequacy and completeness of the design and development of the software. Reviews are performed by peers who have an equivalent knowledge of the topic, but who did not directly generate the software code. Test documentation prepared per SQAP and SVVP requirements are independently reviewed. Problem reporting and corrective action procedures span the entire software life cycle as identified in the SPM and SQAP. The safety I&C systems software configuration management is provided for software version control, logs, access, and physical storage of media.

Software QA audits are performed to ensure that software documentation and processes comply with the standards and guidelines established for the project.

Table 5.3-1 Software Tasks and Responsibilities

TS

TS

5.4. Software Design Process

This section describes the software engineering life cycle for safety I&C systems. The software development process for original software is shown in Figure 5.4-1, which shows the relationship between software and hardware, the process of software design, integration and testing throughout the software life cycle.

Software quality is assured through the process of verification reviews, validation testing at the different phases of development. Verification is the process of determining whether the product of a given phase of software development cycle fulfills the requirements imposed by the previous phase. Validation is usually accomplished by testing and evaluation of the completed software to ensure compliance with the user needs and requirements. Software configuration management is performed during all phases of software development.

Software V&V activities are governed by SVVPs prepared for the integrated software of each system. Required test procedures and test reports are based on the level of the test and the class of the software.

Typical software development and V&V process are as follows:

a. Concept phase (acquisition, planning, and concept)

During this phase, SMP, SQAP, SVVP, SCMP, SDP, SIntP, SInstP, etc. and coding standard are developed.

This phase defines the requirements and the key design aspects for all systems that are critical to the plant's design basis for safety, performance and maintainability. This phase determines the industry regulations and standards that apply to the system and the design process for those systems.

b. Requirements phase
During this phase, two kinds of requirements specification are developed. The first is functional (or system) requirements specification and the second is software requirements specification.

c. Design phase
During this phase the basic platform hardware is manufactured and configured in cabinets with all power and signal wiring. The software design description (SDD) gives a precise description of all the application software for all controllers and HSI devices. Also operations and maintenance manuals are created.

d. Implementation phase
Original software development and modifications to existing software begins with module coding by the software design team (DT) in accordance with the appropriate coding standards. Existing software which has been qualified may be integrated into the software system and tested during this phase. Verifications of code listings are performed. Module/unit testing shall be performed in accordance with test plan.

e. Test phase
During this phase basic software and application software are integrated with the platform hardware for each system. And the software product is evaluated to determine whether or not requirements have been satisfied. The test phase for systems covers software Integration testing and validation testing. Test

procedures and reports shall be documented and verified. Operations and maintenance manuals are also validated during this phase.

f. Installation and checkout phase

Activities in this phase are installation check and commissioning. During this phase controllers are connected with field equipments such as detectors and actuators. Pre-operational tests are conducted to ensure all equipment has not been damaged during shipping or installation and that all interconnections are correct.

g. Operations and maintenance phase
During this phase the safety system is in operation. Self-diagnostics continuously monitor performance and calibration and manual tests are conducted periodically. Failed equipment is replaced.

Software modifications are approved, documented, verified and validated, and controlled in the same manner performed in the design, implementation and test phase.

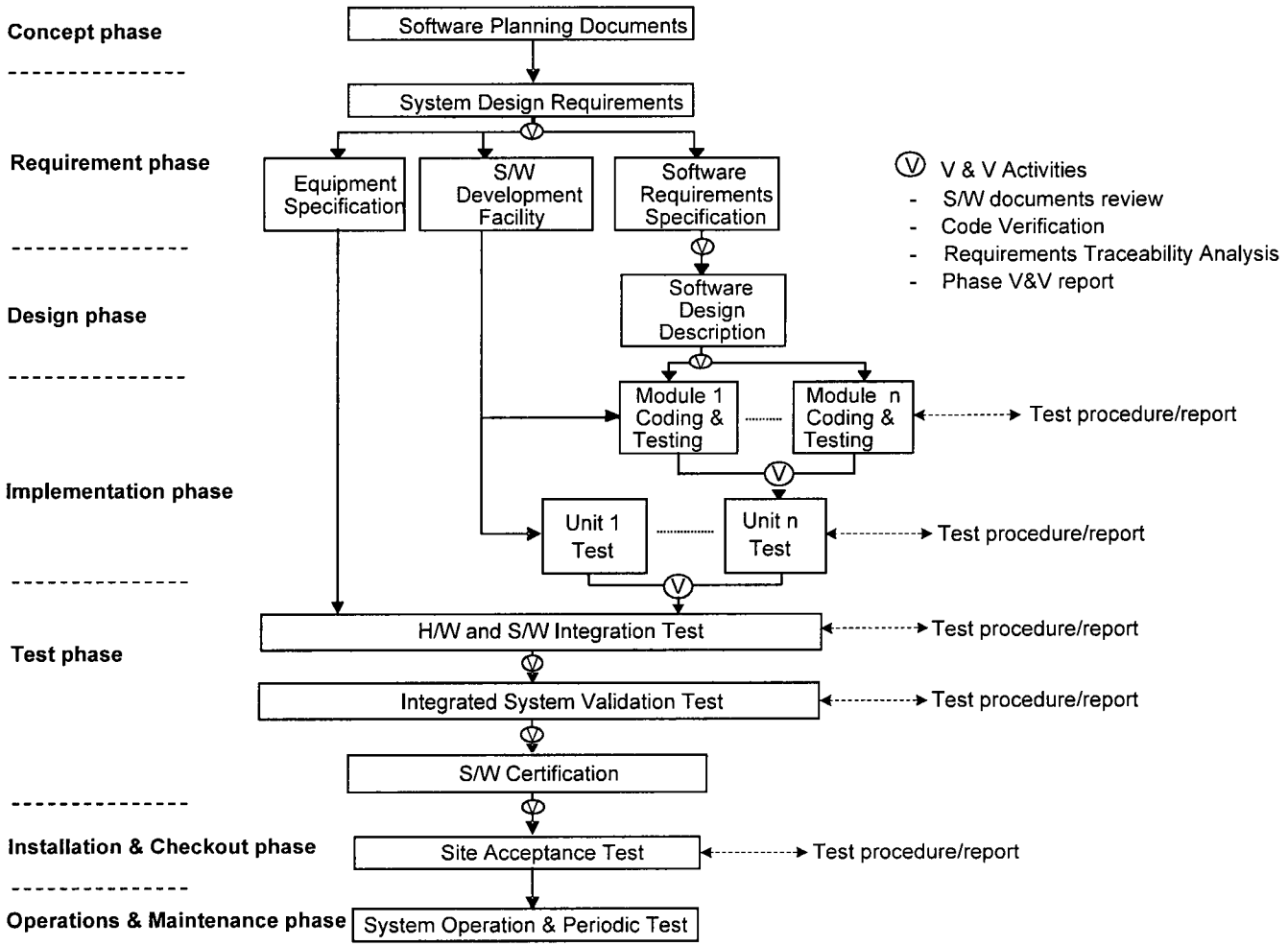


Figure 5.4-1 Simplified Software Life Cycle and Activities

5.5. Software Verification and Validation

This section describes the various software V&V methodologies aimed to increase the system reliability and availability of the safety I&C systems. A SVVP is used, which encompasses safety I&C systems. The V&V methodologies employ systematic checks for detecting errors in the system hardware and software, during each system development and implementation process for Protection and ITS software.

The goals of the V&V plan, when applied to the safety I&C systems, are to:

- Improve the system reliability and availability,
- Expose errors as early as possible to minimize rework,
- Provide a systematic process of objectively evaluating the system performance,
- Demonstrate compliance with system requirements, industry standards and licensing requirements.

The V&V processes start with the system requirements phase and include all necessary V&V activities to verify and/or validate the software.

The verification process checks the results of the phase-by-phase development to determine that there is an accurate translation of one stage (such as design) into the next stage (such as implementation).

The validation process ensures the conformance of the system performance and the system design requirements. Thus, it provides the overall assurance that the capabilities specified in the system design requirements are implemented in the hardware and software, and the system is properly integrated. Another goal is to ensure that problems or potential deficiencies that may have occurred during the design and implementation phase have been corrected.

The initial V&V activity is the review of system design requirements prior to any detailed design of hardware or software. Verification activities are performed at the end of this phase and each subsequent phase. These activities determine that all requirements have been properly transferred from the input products to the output products of the phase, with amplifications or modifications appropriate to the phase. Upon completion of the software implementation, validation activities are performed. These activities determine that the operation of the system is consistent with the system requirements. Thus V&V activities are integrated with project activities from the beginning to the end.

The V&V team is organized independent of those responsible for the design as shown in Figure 5.5-1.

TS

[ ]

Figure 5.5-1 Software Design and V&V Team Organization

The QA team conducts independent audits on the DT and VT activities to confirm that requirements and implementation of the application software lifecycle process are appropriately planned and executed in accordance with the QAM.

5.6. Software Configuration Management

The SCMPs describe the process for identifying, collecting and controlling the complete set of software items associated with each system. Each plan identifies software configuration items, invokes controls on the process of making changes to software, and records and reports on the status of changes. The SCM is intended to be utilized throughout the entire life cycle, including requirements phase, design phase, implementation phase, test phase, installation & checkout phase, operation and maintenance phase, and retirement phase.

The SCMPs are based on industry codes and standards which address the need to:

- Identify sets of software items that compose the system (baseline), including revision level, test status and history, and readiness for release.
- Record and document work in progress on each software item.
- Maintain the association among software documents, code and data.
- Maintain an association between software problem/change reports, affected documentation, and program/data items.
- Implement appropriate controls and approvals for changes to the software configuration.
- Identify the organization responsible for the SCM.
- Provide a backup program for the software (in progress or completed) to protect against loss.

The SCM processes are administered by the software design team leader, using a Librarian and a configuration control system to store, retrieve, catalog, and manage multiple revisions of the software items.

5.7. Commercial Grade Dedication of Predeveloped Software

The commercial grade dedication (CGD) guidance provided in EPRI TR-106439 involves identifying the critical characteristics of the commercial grade digital equipment based on the safety-related technical and quality requirements, selecting appropriate methods to verify the critical characteristics to enable dedication of the digital equipment.

EPRI TR-106439 identifies three categories of critical characteristics in terms of physical, performance, and dependability attributes. These characteristics correspond to the categories identified in IEEE Std. 7-4.3.2.

Verification of the critical characteristics is at the heart of the dedication process.

EPRI TR-106439 adapts four acceptance methods to establish an approach to verify the characteristics for digital equipment. The four methods are as follows:

- Method 1 --- Special tests and inspections
- Method 2 --- Commercial grade survey of supplier
- Method 3 --- Source verification
- Method 4 --- Acceptable supplier/item performance record

6. EQUIPMENT QUALIFICATION

The objective of equipment qualification is to demonstrate that the safety I&C systems equipment is capable of performing its designated safety-related functions during and following a DBE.

Equipment qualification is composed of three (3) major components: environmental, seismic and electromagnetic compatibility (EMC) qualification.

6.1. Environmental Qualification

The safety I&C systems equipment is qualified to meet the requirements of IEEE Std. 323-2003, as augmented by RG 1.209. Since this equipment is located in the mild environments (MCR and/or I&C equipment rooms) where qualified heating, ventilation, and air conditioning (HVAC) is provided, the qualification is performed by a heat rise test and a subsequent analysis using linear temperature data extrapolation.

The tests are performed with the cabinet/enclosure energized to obtain temperature heat rise data at various locations within the cabinet assembly. Temperatures are monitored until they are stable within the cabinet with its doors and cable entrance areas closed. Then by linear extrapolation, the internal temperature profile based on a change in the external ambient temperature is determined.

The analysis demonstrates, using extrapolated test data, that individual component and equipment temperature specifications are not exceeded within the cabinet/enclosure when exposed to the environmental conditions as specified in Table 6.1-1.

6.2. Seismic Qualification

The safety I&C systems equipment is qualified by test, analysis or a combination of both methods in accordance with IEEE Std. 344-2004, as endorsed by RG 1.100. Functional operability tests will be conducted during seismic qualification tests with the equipment energized and using simulated inputs and interfaces.

The safety I&C systems are designated as Seismic Category I in accordance with RG 1.29. It is designed and qualified to withstand the cumulative effects of five (5) 1/2 Safe Shutdown Earthquakes (SSEs) followed by one SSE without loss of safety functions and physical integrity. The 1/2 SSE and SSE at the safety I&C systems cabinet and OM mounting points are characterized by the required response spectra , which envelope the I&C equipment room and MCR SC.

The safety I&C systems electro-mechanical components that have significant aging mechanism, such as relays, will be cycled to the end of operational life condition prior to qualification.

The seismic tests and/or analysis demonstrate that:

- During the seismic events, no parts of the equipment will loosen, bend or crack in a manner that impairs proper operation. In addition, no parts of the equipment will become a missile hazard.
- During and after the seismic event, the safety-related parameters of the equipment will be maintained.

Table 6.21-1 Environmental Design Requirements

Environmental Parameter	Normal		
	Min.	Max.	Duration
Safety I&C System Cabinets in I&C Equipment Room			
Temperature	70 °F	77 °F	Continuous
Humidity	40 %RH	60 % RH	Continuous
Pressure	Atmospheric		Continuous
Radiation	10 Gy Gamma (3)		Continuous
Operator Module in the MCR SC			
Temperature	70 °F	95 °F	Continuous
Humidity	40 %RH	60 % RH	Continuous
Pressure	Atmospheric		Continuous
Radiation	10 Gy Gamma (3)		Continuous

Notes:

(1) Relative humidity is based on standard temperature and pressure of 70 °F and 0 psig.

(2) Includes an 18 °F temperature rise within the MCR SC.

(3) Total integrated doses over equipment life time (40 years)

6.3. EMI/RFI Testing

The safety I&C systems equipment is qualified in accordance with MIL Std. 461E and IEC 61000 Part 4 Series as augmented by RG 1.180. EMC testing of the equipment will be performed for both conducted and radiated signals as follows:

- EMI/RFI emissions
- EMI/RFI susceptibility / immunity
- Surge withstand capability

The tests are performed on each system in various modes of operation such that successful completion of the test demonstrates that the safety system function has not been compromised and the equipment performs within its design specifications.

When conducting EMC equipment qualification, the test equipment represents the as-delivered configuration. The equipment grounding and power line filter are identical to the tested equipment.

The basis for selecting the specific tests and operating envelops (test level, applicable frequency and limitations) is based on RG 1.180.

7. EQUIPMENT RELIABILITY

The safety I&C systems configurations are designed for high reliability using PLC equipment . The reliability (availability) of these system configurations to perform their safety functions, using the SFC, is demonstrated via the failure modes and effects analyses (FMEAs).

7.1. Failure Modes and Effects Analysis (FMEA)

The FMEA is a "qualitative" evaluation which identifies various failure modes that can occur to the components that compose a system. It is not a "Quantitative" reliability / availability analysis which produces calculated numerical values. The FMEA identifies significant single failures and their effects or consequences on the system's ability to perform its functions. The system level FMEA is provided in the DCD.

The FMEA is performed for protection systems' sensors, and bistable/coincidence and actuating logics. The FMEA is prepared conservatively assuming that one PPS channel is already bypassed for maintenance.

At the hardware interface level for all computers, the FMEA bounds all cases by considering the worst case effects at the computer outputs. For binary outputs, open and closed statuses are addressed. For digitized data, interfaces are analyzed for failure to transmit data, failure to receive data and communication of erroneous data.

The safety I&C systems are designed so that any single failure will not prevent proper protective action at the system level. The FMEA shows that no single failure will prevent the systems from performing their protective functions.

The FMEA addresses all credible failures from each system's computers (e.g. communications failures, stalls, etc.); not all possible causes of the failure condition. At the hardware interface level, the FMEA considers the failure modes of all components from the input circuits to the output circuits, including all intermediate circuits and components, which process the system information/data.

The FMEA is typically documented in tabular format which includes the following table entries:

- Element no.: Sequential number assigned to element/module/component
- Name: Element/module/component descriptive name
- Failure mode: Significant failure mode description: such as high/low output, on/off, open/closed, tripped/ not tripped, no data output, etc.
- Cause: Most predictable cause of associated failure mode listed such as:
  - External input/output circuits/cabling (open/shorted)
  - Mechanical failure
  - Vital instrument power buses (off/open/shorted/grounded)
  - Internal AC/DC power supplies (off/open/shorted)
  - Input and output modules (fail off/on/high/low/as-is)
  - PLC modules (fail off/on/stalls)

- Data communications modules (fail off/transmit/ receive/as-is)
- Software (fails off/stalls/spurious data)
- Fiber optic receiver/transmitter modules (off/open/shorted)
- Relay coils/contact (open/shorted)
- Manual switches (open/shorted)

- Symptoms and local effects: Identifies the immediate consequence of each failure mode and any secondary side effects.
- Method of detection: Identifies method by which failure is detected, e.g.: self annunciating, automatic or manual test, etc.
- Inherent compensating provisions: Any compensating features within the design are addressed such as:
  - Redundant channels of PPS and ESF-CCS
  - Auctioneered AC/DC power supplies
  - Fail-safe design

  For example, outputs go to appropriate trip, initiation or actuation state upon loss of electrical power.
  - Fail-safe design upon loss of data communications

  For example, credible data communications network failures (due to communication module, interconnecting coaxial or fiber optic cable failure, etc.) result in detection of the loss of data communications by the receiving PLC processor on its network. Upon detection of the loss of communications, the effected processor will force its safety-related trip output signals to their "fail-safe" state.
- Effect on system: Describes the ultimate effect of the failure mode on the overall system, e.g.: logic is changed from 2-out-of-4 to 2-out-of-3 coincidence or ESFAS function is actuated.
- Remarks and other effect: Identifies the effects of the failure on overall plant operations or interfacing systems.

The FMEA considers the effects of these types of failures on the system and any other impacts on interfacing plant systems or components.

The system level FMEA results of the PPS and ESF-CCS are included in the DCD. The FMEA is performed based on replaceable module level.

7.2. Unavailability Analysis

An unavailability analysis is performed on both the PPS and the ESF-CCS to assess their unavailability when they are requested to perform their function. The analysis quantifies the probability that the PPS would fail to trip the reactor upon demand. The analysis also quantifies the probability that ESF-CCS would fail to actuate safe guard equipment when demanded.

The fault tree model for the PPS and ESF-CCS design is developed to perform this analysis. The PPS and ESF-CCS fault tree contains failures or faults which could render the affected system unavailable given a demand for the system to perform its specified function.

8. REFERENCES

[1] Diversity and Defense-in-Depth Technical Report

[2] Setpoint Methodology for Plant Protection System

[3] Uncertainty Methodology and Application for Instrumentation

[4] Technical Report for Software Program Manual

[5] CCF Coping Analysis Technical Report

[6] Quality Assurance Manual

[7] Design Control Document for APR1400

APPENDIX A CONFORMANCE TO IEEE STD. 603-1991

This Appendix describes how the safety I&C systems satisfy the requirements of IEEE Std. 603-1991. The APR1400 is an advanced nuclear power plant and includes computer based safety I&C systems. Therefore, the 1998 edition of IEEE Std. 603 is incorporated to address the digital I&C system design criteria such as EMI/RFI testing and CCF analysis. The following heading numbers with "A" correspond to the section numbers of IEEE Std. 603-1991.

A.1 Scope

The safety system criteria contained in IEEE Std. 603 are applicable to the PPS and ESF-CCS, which initiate safety actions to mitigate the consequences of design-basis events. It is also applicable to those parts of DCSs that support safety system functions.

A.2 Definitions

There is no exception in the PPS and ESF-CCS designs.

A.3 References

The PPS and ESF-CCS conform to all referenced codes and standards.

A.4 Safety System Designation

The design of the PPS and ESF-CCS is based on a set of specific design bases as follows.. (the head number is consistent with the subsection number in Section 4 of IEEE Std. 603-1991).

1. The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event:

   The RPS is designed to ensure adequate protection of the fuel, fuel cladding, and RCS boundary during AOOs.

   In addition, the system is designed to assist the ESF Systems in mitigating the consequences of accidents.

   Each DBE is described in Chapter 15 of the DCD.

   The allowable limit for each design basis event and accident is described in Chapter 15 of the DCD.

2. The safety functions and corresponding protective actions of the execute features for each design basis event:

   The safety functions and corresponding protective actions for design basis event stated in item a) are as follows:.

   The RPS consists of fifteen trips in each of the four RPS channels that will initiate the required automatic protective action utilizing a coincidence of two like trip signals.

   a) Variable Overpower Trip

      (a) Input

         Neutron flux power from the ENFMS.

      (b) Purpose

         To provide a reactor trip to assist the ESF systems in the event of an ejected CEA accident.

   b) High Logarithmic Power Level Trip

      (a) Input

         Neutron flux power from the ENFMS.

      (b) Purpose

         To ensure the integrity of the fuel cladding and RCS boundary in the event of unplanned criticality from a shutdown condition, resulting from either dilution of the soluble boron concentration or uncontrolled withdrawal of CEAs.

         If CEAs are in the withdrawn position, automatic trip action will be initiated. If all CEAs are inserted, an alarm is provided to alert the operator to take appropriate action in the event of an unplanned criticality.

   c) High LPD Trip

      (a) Inputs

         Neutron flux power and hot pin axial power distribution from the ENFMS.

         Radial peaking factors from CEA position measurement system (reed switch assemblies).

         ΔT power from coolant temperatures, pressure and flow measurements.

         PFs from CEACs for CEA deviation within a subgroup.

         PFs generated within the CPC for subgroup deviation and groups out-of-sequence.

      (b) Purpose

         To prevent the linear heat rate (W/cm or kW/ft) of fuel pin in the core from exceeding fuel design limits in the event of AOOs.

   d) Low DNBR trip

      (a) Inputs

         Neutron flux power and hot pin axial power distribution from the ENFMS.

RCS pressure from PZR pressure measurement.

ΔT power from coolant temperatures, pressure and flow measurements.

Radial peaking factors from CEA position measurement (reed switch assemblies).

Reactor coolant mass flow from reactor coolant pump speeds and temperatures.

Core inlet temperature from reactor coolant cold leg temperature measurements.

PFs from CEACs for CEA deviation within a subgroup.

PFs generated within the CPC for subgroup deviation and groups out-of-sequence.

(b) Purpose

To prevent the DNB ratio of the coolant channel in the core from exceeding the fuel design limit in the event of AOOs. In addition, this trip will provide a reactor trip to assist the ESF systems in limiting the consequences of the steam line break outside containment, S/G tube rupture and reactor coolant pump shaft seizure accidents.

e) High PZR Pressure Trip

(a) Input

Reactor coolant pressure from narrow range PZR pressure measurement.

(b) Purpose

To assure the integrity of the RCS boundary for any defined AOO that could lead to an over pressurization of the RCS.

f) Low PZR Pressure Trip

(a) Input

Reactor coolant pressure from wide range PZR pressure measurements.

(b) Purpose

To provide a reactor trip to assist the ESF systems in the event of reduction in system pressure and a LOCA

g) Low S/G Water Level Trips

(a) Input

Level of water in each SG downcomer region from wide range differential pressure measurements.

(b) Purpose

To provide a reactor trip to assist the ESF systems ensuring that there is sufficient time for actuating the auxiliary feedwater pumps to remove decay heat from the reactor in the event of a reduction of S/G water inventory.

h) Low S/G Pressure Trips

(a) Input

Steam pressure in each SG.

(b) Purpose

To provide a reactor trip to assist the ESF systems in the event of a steam line break accident.

i) High Containment Pressure Trip

(a) Input

Pressure inside containment.

(b) Purpose

To assist the ESF systems by tripping the reactor coincident with the initiation of safety injection caused by excessive pressure in containment.

j) High S/G Water Level Trips

(a) Input

Level of water in each SG downcomer region from narrow range differential pressure measurements.

(b) Purpose

To assist the ESF systems by tripping the reactor coincident with initiation of main steam isolation caused by a high SG water level.

k) Low Reactor Coolant Flow

(a) Input

Pressure differential measured across the S/G primary side.

(b) Purpose

To provide a reactor trip in the event of a reactor coolant pump sheared shaft.

l) Manual Reactor Trip

(a) Input

Two independent pairs of trip pushbuttons are provided at MCR and one set of trip pushbuttons in the RSR consoles.

(b) Purpose

Manual reactor trip is provided to permit the operator to trip the reactor.

3. The permissive conditions for each operating bypass capability that is to be provided:

The RPS operating bypass types (name and function), permissive and removal condition are described in Table 7.2-1 of the DCD.

The ESFAS operating bypass types (name and function), permissive and removal condition are described in Table 7.3-1 of the DCD.

4. The variables or combination of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action:

The monitored variables are provided in Table 7.2-4. of the DCD.

The RPS monitors the following generating station conditions in order to provide adequate protection during AOOs:

a) Core power (neutron flux)

b) Reactor coolant system pressure

c) DNBR in the limiting coolant channel in the core.

d) Peak local power density in the limiting fuel pin in the core

e) S/G water level

f) Reactor coolant flow

The RPS monitors the following generating station conditions in order to assist the ESF in mitigating the consequences of accident:

a) Core power

b) RCS pressure

c) S/G pressure

d) Containment pressure

e) Reactor coolant flow

The system is designed so that protective action will not be initiated during normal operations. The selection of these trip setpoints is such that adequate protection is provided, since all sensor and processing time delays and inaccuracies have been taken into accounts. Reactor trip delay times and analysis setpoints used in the Chapter 15 are given in Table 7.2-7 and Section 15.0-2 of the DCD.

The reactor protection system sensor response times, reactor trip delay times, and analysis setpoints used in Chapter 15 of the DCD are representative of the manner in which the RPS and associated instrumentation will operate. These quantities are used in the transient analysis documented in Chapter 15 of the DCD. Actual RPS equipment uncertainties, response times and reactor trip delay times are obtained from calculations and tests performed on the RPS and associated instrumentation. The verified system uncertainties are factored into all RPS setpoints to ensure that the system works as intended when the errors and uncertainties combine in a conservative manner.

5. The following minimum criteria for each action whose operation may be controlled by manual means initially or subsequent to initiation:

5.1. The point in time and the plant conditions during which manual control is allowed.

Manual control is not permitted within 30 minutes of an accident occurring. The assumption, initial condition, event details and plant state for each accident and event is described in Chapter 15 of the DCD. Manual control after RPS initiation is performed according to emergency operation procedure for plant state.

5.2 The justification for permitting initiation or control subsequent to initiation solely by manual means.

The RPS is not designed to permit initiation only by manual means.

5.3 The range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed.

MCR environmental conditions during manual operation are described in Section 6.4 of the DCD.

5.4 The variables in item d that shall be displayed for the operator to use in taking manual action.

The variable list in item 4) that shall be displayed for the operator for taking manual action is described in Table 7.5-1 of the DCD.

6. For those variables that have a spatial dependence, the minimum number and locations of sensors required for protective purpose:

The number, and location of the sensors provided to monitor those variables in item 4) are given in Table 7.2-3 of the DCD. The location of precision RTD for measuring RCS hot leg temperature is assigned to measure appropriate coolant transmission effects by temperature difference and temperature distribution of hot leg.

7. The range of transient and steady state conditions of both motive and control power and the environment during normal, abnormal, and accident conditions throughout which the safety system shall perform:

The RPS is qualified to meet environmental conditions in Section 3.11 of the DCD, in accordance with IEEE 323. In addition, the system is capable of performing its intended function under the most degraded conditions of the energy supply, as addressed in Section 8.3 of the DCD.

8. The conditions that could cause functional degradation of safety performance and for which provisions shall be incorporated to retain the capability for performing the safety functions:

The RPS logic design takes account of functional degradation that could occur in the following conditions:

a) System actuation due to the power loss of measurement channel

b) Appropriate system level protective action due to single accident in system

c) The RPS is verified according to IEEE 344 to demonstrate that the RPS can perform the intended function for seismic conditions.

d) The RPS is verified according to IEEE 323 to demonstrate that the RPS can perform the intended function for environment conditions.

e) System components are qualified according to an established plan for EMC that requires the equipment to function properly when subjected to electrical surges, electromagnetic interference, radio frequency interference, and electrostatic discharge. Qualification is applied in equipment based on operating environment and/or inherent design characteristics. Electromagnetic interference

qualification is performed in accordance with RG 1.180 and IEC 61000-4-2. Radiated and conducted electromagnetic interference envelopes are established for qualification.

9. The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design:

   The reliability of RPS is described in Table 7.2-5 of the DCD.

10. The critical points in time or the plant conditions, after the onset of a design basis event, including:

    10.1 The points in time or the plant conditions for which the protective actions of the safety system shall be initiated.

    The point, for which the reactor shutdown shall be initiated (trip setpoint) is described in Table 7.2-4 of the DCD, and initial event and frequency causing initiation of protective action are described in Table 15.0-3 of the DCD.

    10.2 The points in time or the plant conditions that define the proper completion of the safety function

    The point in time for the proper completion of RPS safety function is when CEA is injected completely into the core.

    In this time, plant maintains the following conditions.

    Core reactivity maintains the subcritical state with sufficient margin corresponding to technical specification and, does not exceed thermal design limit of core and reactor coolant system by removing core decay heat at controlled cooling rate.

    The vital equipment and system operates within design range for maintaining the above conditions.

    The equipment and system for maintaining offsite dose within an acceptable limit are operating appropriately.

    10.3 The points in time or the plant conditions that require automatic control of protective actions

    The accident analysis in Chapter 15 of the DCD does not consider manual control in the first 30 minutes after accident and the point in time (RPS trip set point (Table 7.2-4)) for automatic control of protection system is set based on accident analysis results. Automatic initiation is required for maintaining item 10.2 condition when reaching setpoint.

    10.4 The points in time or the plant conditions that allow returning a safety system to normal

    When the plant operates in condition of 10.2 above returning a safety system to normal is allowed.

11. The equipment protective provisions that prevent the safety systems from accomplishing their safety functions:

There is no equipment protective provisions that prevent the safety systems from accomplishing their safety functions.

12. Any other special design basis that may be imposed on the system design (example., diversity, interlocks, regulatory agency criteria):

The system is designed to reduce the failure of redundant channels anticipated by CCF.

A.5 Safety System Criteria

A.5.1 Single-Failure Criterion

The BP in PPS provides their trip signals to the LCL processor located in the four redundant channels. The local coincidence logic processors determine the local coincidence logic trip based on the state of the four like bistable trip signals and their respective bypasses. Single failures at the coincidence logic level are accommodated by either redundancy within each channel or redundancy across the four channels. The coincidence trip signals are used in the generation of the RTSS or ESF-CCS initiation. The PPS is designed so that any single failure within the system shall not prevent proper protective action at the system level, even when a channel is intentionally bypassed for test or maintenance. No single failure will defeat more than one of the four protective channels associated with any one trip function.

Single failure of RTSG is accommodated by the full 2-out-of–4 arrangement of the devices. A spurious opening of a RTSG does not result in either spurious trip or loss of ability to trip.

The ESFAS initiation signals from the PPS are sent to separate ESF-CCS cabinets. Each cabinet contains the actuation logic for only one channel; therefore, a failure in one cabinet cannot affect the circuitry and actuated equipment of the other divisions.

Single failures of the actuation (or control) logic will cause, at worst, only a failure of a component, group of components, or one entire redundant train; actuation of the remaining redundant channels is sufficient for the protective action.

The wiring in the system is grouped so that no single fault or failure, including either an open or shorted circuit, will negate protective system operation. Signal conductors and power leads coming into or going out of each cabinet are protected and routed separately for each channel of each system to minimize possible interaction.

Single failures considered in the design of the PPS and ESF-CCS will be described in the FMEA in the DCD.

A.5.2 Completion of Protective Action

The system is designed to ensure that protective action such as RPS and ESFAS will go to completion once initiated. Operator action is required to clear the trip (or initiation) and return to operation.

RPS function is initiated when the reactor TCBs open. Protective action is completed when the CEAs arrive at their full-in position.

ESFAS function is initiated when the 2-out-of-4 logic in PPS is met. A protective action is completed when all of the appropriate ESF-actuated components have assumed the proper state for their ESF function.

The ESF components remain in the actuated safe state until the ESF system level actuation signal is manually reset after the trip condition in PPS is cleared.

A.5.3 Quality

Components and modules in PPS and ESF-CCS have a quality that is consistent with minimum maintenance requirements and low failure rates. PPS and ESF-CCS is designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANSI/ASME NQA1-1989).

A.5.4 Equipment Qualification

Equipment qualification (environmental, seismic and EMI/RFI qualification) of the PPS and ESF-CCS is described in Section 6 of this report.

A.5.5 System Integrity

Type testing of components, separation of sensors and channels, and qualification of the cabling are utilized to ensure that the channels maintain their functional capability required under applicable extremes of environment, power supplied, malfunction, and DBE conditions.

Loss of any one channel will not prevent the protective action of the PPS and ESF-CCS. Sensors are connected so that blockage or failure of any one connection does not prevent protective system action. The process transducers located in the containment building are specified and rated for the intended service. Components that must operate during or after a limiting fault (postulated accident) are qualified for the most limiting environment for the period of time for which they must maintain their functional capability. Results of type tests are used to verify this.

The system response time test is performed before and after installation to ensure to complete protective function within predefined time. The PPS and ESF-CCS meet the requirements of IEEE 7-4.3.2 for design considering computer system integrity, test and calibration. When the critical failure of hardware and software detectable by diagnostic function occurs, the PPS and ESF-CCS generate initiation signal or annunciation system. The PPS provides alarms to the QIAS-N and IPS to indicate system abnormalities.

The PPS restarting will set all outputs to trip or initiation condition and the ESF-CCS to non-actuated condition. These initial conditions are maintained until the application program is executing properly.

The test and maintenance equipment such as MTP/ITP is designed not to affect processor performing safety function.

The PPS and ESF-CCS software including software development, verification and validation, testing and configuration management meets the requirements in the SPM.

A.5.6 Independence

A.5.6.1 Between Redundant Portions of a Safety System

The PPS and ESF-CCS cabinets for each channel are geographically distributed into four separate channelized I&C equipment rooms.

The routing of Class 1E and associated cabling and sensing lines from sensors meet the requirements of RGs 1.75 and 1.151.

This requires that the cabling for the four safety channels be routed separately; however, the cables of different safety functions within one channel may be routed together. Low energy signal cables are generally routed separately from all power cables. Safety-related sensors are separated. The separation of safety-related cables requires that the cables be routed in separate cable trays. Associated circuit cabling from redundant channels is handled the same as Class 1E cabling.

The PPS and ESF-CCS channel receives non-interrupt AC power from Vital Bus Power Supply System. The PPS and ESF-CCS do not share the power between channels for electrical separation and isolation.

Cabling associated with redundant channels of safety-related circuits is installed such that a single credible event cannot cause multiple channel malfunctions or interactions between channels.

Redundant portions of the PPS and ESF-CCS are independent from one another so that a failure in any one portion of the system does not prevent the redundant portions from performing the RPS and ESFAS function.

LCL in PPS and GC in ESF-CCS receive the signals from redundant channel through fiber optic modem and cable for maintaining the electrical isolation.

Refer to Appendix C for communication independence between channels.

A.5.6.2 Between Safety Systems and Effects of Design Basis Event

Independence between the components of the PPS and ESF-CCS and the effects of design-basis event is provided by qualifying the equipment in accordance with the requirements in Section 6 of this report.

A.5.6.3 Between Safety Systems and Other Systems

Non-Class 1E instrumentation circuits and cables (low level) which may be in proximity to Class 1E or associated circuits and cables, are treated as associated circuits unless analyses or tests demonstrate that credible failures therein cannot adversely affect Class 1E circuits.

Associated circuits provide the supporting function including annunciation, test and communication, which are not related to class 1E function.

Outputs from the safety system to non-safety-related areas are isolated utilizing fiber optic cable so that a failure in the non-safety-related area does not cause loss of the safety system function. The signals originating in the MTP/ITP which feed the IPS/QIAS-N are isolated utilizing fiber optic cable to maintain their channel independence.

Data flow is unidirectional from Class 1E systems to non-Class 1E system. Separate communication processors are utilized to protect the Class 1E functional processors from handshaking and data communication errors.

Qualification for the potential effect on Class 1E systems of communication errors caused by hardware failure or software error originating in non-Class 1E systems is an integral part of software verification and validation for all Class 1E systems. Validation test methods are developed on a case-by-case basis and are based on the software, hardware and data protocols in use.

Refer to Appendix C for communication independence between safety system and non-safety system.

A.5.6.4 Detailed Criteria

Each redundant channel is independent of the other redundant channels. The sensors are separated, cabling is routed separately and each redundant channel is located in a separate cabinet. This minimizes the possibility of a single event causing more than one channel's failure. The outputs from these redundant channels are isolated from each other so that a single failure does not cause impairment of the system function.

Within the RPS, functional and software independence is maintained between PPS channels for trip functions by using fiber optic cables for CCC SDL for redundant channels.

The details for communication independence are described in Section 4.0 and Appendix C of this report.

A.5.7 Capability for Test and Calibration

The PPS and ESF-CCS design complies with IEEE Std. 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems", and RG 1.22, "Periodic Testing of Protection System Actuation Functions".

The PPS incorporates continuous system self-checking features that minimize required manual surveillance and periodic testing. System self-checking features include on-line diagnostics for the computer system, hardware, and the communications systems.

Provisions for periodic manual surveillance testing provide the overlapped testing functions that confirm operability of each hardware module in the system and specifically determine operability of any hardware components that are not tested by the system's self-diagnostics.

Manual surveillance testing verifies that the hardware components and connections have not failed or degraded and trip signal path including application program for safety functions is correct. Software itself does not "degrade" over time unless there is an associated hardware failure. Also, V&V confirms that the software is correct. Therefore, software testing is not performed by surveillance testing. The diagnostic functions check the hardware integrity and supervise the program by cyclic redundancy checksum (CRC) comparison.

The MTP displays test feedback for redundant channel through ITPs via the SDLs.

The PPS bypasses are initiated via channel bypass switches on the MTP switch panel.

The response time is verified by measurement during plant startup testing. Sensor responses are measured during factory or laboratory testing and provided to the site operator for use in the test program.

A.5.8 Information Display

Means are provided to allow the operator to monitor all trip or actuation system inputs, outputs, and calculations.

A.5.8.1 Displays for Manually Controlled Actions

Indication of test or bypass conditions, or removal of any PPS channel from service is given by the OM, QIAS-N and IPS displays. The PPS operating bypass status information is provided including automatic operating bypass removal.

The QIAS-P provides a continuous and dedicated display of RG 1.97 Type B,C variables including the ICCM variables. Type A variables are displayed by conventional indicator.

The QIAS-N provides the information required for EOP execution, safe shutdown, critical operator action and technical specification (TS) monitoring to be used during/after plant accident condition.

The DIS provides the diverse displays from the QIAS-P and QIAS-N.

A.5.8.2 System Status Indication

System status indication is provided for all protective actions at the OM, IPS and MTP, including identification of channel trips.

A.5.8.3 Indication of Bypasses

The operating bypass and trip channel bypass status is available for display at the IPS display and OM FPD in the MCR and MTP in the I&C equipment room.

A.5.8.4 Location

Status information including input variable value, setpoint, trip, pre-trip, initiation, trip channel bypass and operating bypass is displayed on the IPS display and OM FPD in the MCR and MTP in the I&C equipment room.

A.5.9 Control of Access

Trip channel bypasses are administratively controlled. When the first channel is bypassed, there is an audible and visible alarm to indicate which channel is being bypassed. The specific parameter or parameters being bypassed are indicated at the MTP and OM.

The operating bypasses have audible and visible alarms. The operating bypasses have automatic features that provide a permissive range at which they can be actuated. Should the permissive range be exceeded, the bypass will be automatically removed.

Operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing. The following operating bypasses are provided:

- High Logarithmic Power Level Bypass
- High LPD and Low DNBR Bypass
- Low PZR Pressure Bypass
- CPC-CWP Bypass

Keys or built-in features are provided to control setpoints, calibration, and test point adjustments. Access is indicated to the operator. Access is controlled via key locks, administrative procedures, and other means to limit access.

A.5.10 Repair

Identification of a defective input channel will be accomplished by observation of system status indication or by testing. Replacement or repair of components is accomplished with the affected input channel bypassed.

The affected trip function then operates in a 2-out-of-3 trip logic while maintaining the coincidence of two required for trip or actuation.

For the 1-out-of-2 ESFAS (BOP portion), the affected trip function then operates in single active channel trip logic.

A.5.11 Identification

All equipment, including panels, modules, and cables associated with the trip system, will be marked in order to facilitate identification. Interconnecting cabling will be color-coded.

The physical identification is provided so that an operator can confirm if PPS cabinet, ESF-CCS cabinet, RTSS and related cable are a safety-related system. The PPS and ESF-CCS cabinets are distinguished by name plates. The physically isolated cable from sensor to RTSS is identified by different colors between channels. The color coding is not used for wiring in a same cabinet.

The identification of software is assured by implementing the contents of the SPM.

A.5.12 Auxiliary Features

Auxiliary features (bypass, CWP signal, test and calibration functions) are designed not to prevent the protection system from accomplishing their safety functions.

A.5.13 Multi-Unit Stations

This requirement is not applicable.

A.5.14 Human Factors Considerations

The PPS and ESF-CCS are designed for the operator and maintenance personnel to accomplish their assigned functions successfully during the various plant conditions.

The HSI design for operator and maintenance personnel is designed in accordance with relevant parts of GDC 19 of 10 CFR 50 & 10 CFR 52. Verification and validation activities are performed under the conditions specified in the HFE Verification and Validation (V&V) Plan.

A.5.15 Reliability

The PPS and ESF-CCS reliability is described in Section 7 of this report.

The reliability of software is assured by implementing the requirements of the SPM.

A.6 Sense and Command Features – functional and design requirements

A.6.1 Automatic Control

The design of the PPS and ESF-CCS includes the functions for the automatic control (bistable logic, local coincidence logic, and circuits) in each channel to initiate the required

protective actions. Operator doesn't need to perform any action while the automatic control function is active.

The RTSS circuit breaker is actuated when it receives the automatic reactor trip signals.

A.6.2 Manual Control

Four manual reactor trip switches (per each channel) are provided to permit the operator to trip the reactor. Single failure does not prevent the manual trip function from being performed properly.

All ESF actuation signals including BOP ESFAS can be manually initiated by the operator from the MCR in accordance with procedures.

Manual ESF system level actuation switches are provided for each ESFAS function for SIAS, CIAS, MSIS, CSAS and AFAS.

Subsequent to initiation, each ESF system, including latched portions of AFAS, must be manually reset to restore the initiation logic to the non-actuated state. No single failure will prevent a manual actuation at the system level.

The manual control is not allowed administratively until the actuation setpoint of the PPS is reached. The manual control is carried out in accordance with EOP only when the manual control is required to mitigate the accident at the initiation of protective function.

The Class 1E control means are provided to perform manual actions necessary to maintain the safety condition after completing the protective action automatically by the PPS.

A.6.3 Interaction between the Sense and Command Features and Other Systems

No portion of the PPS is used for both protective and control functions with the following exception: The PPS's low DNBR, high LPD, and high PZR pressure provide a CWP, which is treated as an associated circuit. As an associated circuit, it meets the requirements of IEEE Std. 603-1991.

Signals from the PPS are isolated such that a failure will not affect the protective action of the PPS. The CWP is isolated in the DRCS cabinets to prevent a failure in the DRCS from propagating back into the PPS.

The control and monitoring signals for the PPS from the ENFMS are isolated in the ENFMS prior to being sent. These signals meet the requirement of IEEE384 and Reg.1.75.

A.6.4 Derivation of System Inputs

In so far as is practicable, system inputs are derived from signals that are direct measures of the desired variables. Variables that are measured directly include neutron flux, temperatures, and pressures. Level information is derived from appropriate differential pressure measurements. Flow information is derived from reactor coolant pump speed measurement, S/G differential pressure, and reactor coolant temperature.

A.6.5 Capability for Testing and Calibration

Refer to item "A5.7 Capability for Testing and Calibration".

A.6.6 Operating Bypasses

The operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing.

The operating bypasses have automatic features that provide a permissive range at which they can be actuated. Should the permissive range be exceeded, the bypass will be automatically removed.

A.6.7 Maintenance Bypass

RPS and ESFAS parameters can be bypassed for maintenance. When one channel is in bypass, the coincidence logic in the LCL reverts to 2-out-of-3. The bypass algorithm prohibits more than one channel from being placed in bypass.

The protection functions of the RPS and ESFAS are maintained while the system is bypassed.

A.6.8 Setpoints

The generation of safety system setpoints conforms to ISA-S67.04-1994, "Setpoints for Nuclear Safety Related Instrumentation Used in Nuclear Power Plants."

The environment considered when determining errors is the most detrimental realistic environment calculated or postulated to exist until the worst case time of the required RPS or ESFAS. This environment may be different for different events analyzed. For the setpoint calculation, the accident environment error calculation for process equipment uses the environmental conditions up to the longest required time of trip or actuation that results in the largest errors, thus providing additional conservatism to the resulting setpoints.

The reference leg heating component uncertainties for S/G level also take into account pressure and temperature variation within the S/G.

For all temperature and pressure setpoints, the trip will be initiated at a point that is not at saturation for the equipment. For level setpoints, no analysis setpoint is within 5% of the ends of the level span.

When the pressure (or temperature) reaches to saturation condition, the pressure (or temperature) is not increased by temperature (or pressure). The temperature (or pressure) could not be used for trip parameter in this range. Therefore, the sentence means that the trip shall be initiated before saturation condition.

Analysis setpoint for high level is determined to be less than 95% and analysis setpoint for low level to be more than 5%. This is to protect the equipment considering delay time.

Manual reduction of the setpoints for low PZR pressure and low S/G pressure trips is used for the controlled reduction of PZR pressure and S/G pressure. The setpoint reductions are initiated by the MCR SC pushbuttons for each channel, one pushbutton for the PZR pressure and one pushbutton for both S/G pressures within the channel. This method of setpoint reduction provides positive assurance that the setpoint is never decreased below the existing pressure by more than a predetermined amount.

The variable overpower trip setpoint tracks the actual reactor power from a minimum value to a high value or vice versa, if the power changes slowly enough. The variable overpower trip setpoint is designed with a maximum rate of decrease or increase. If the actual power increases at too rapid a rate, it will catch up with the more slowly increasing setpoint and cause a trip.

The low reactor coolant flow trip setpoint automatically tracks below the input variables by a fixed margin for all decreasing inputs with a rate less than the rate limit. The setpoint decreases at a fixed rate for all decreasing input variable changes greater than the rate limit. If the input variable decreases at too rapid a rate, it will catch up with the more slowly decreasing setpoint and cause a trip. The setpoint automatically increases as the input variable increases.

Refer to the Setpoint Methodology for Plant Protection System (Reference 2) for detailed setpoint methodology.

A.7 Executive Features - functional and design requirements

A.7.1 Automatic Control

The RTSG is operated automatically by automatic reactor trip signal.

The ESF components are activated automatically by the ESF-CCS.

A.7.2 Manual Control

There is manual reactor trip switch in the RTSG. The single failure of a manual reactor trip switch in the RTSG does not prevent manual shutdown function of the PPS.

The RTSG is operated by manual reactor trip switch in the MCR SC or RSR console or pushbutton on the RTSG cabinet.

The ESFAS is actuated by the actuation signals of the manual ESF system level actuation switches on the MCR SC or component control signals generated by the ESCM in the MCR and RSR console.

A.7.3 Completion of Protective Action

The PPS and ESF-CCS are designed to complete the protective action (reactor trip or ESFAS initiation) once it is initiated. An operator's action is required to reset the trip conditions and reactor TCBs before returning to the normal operation condition. Also ESFAS initiation signals are latched (except valve portion of AFAS logic) and require manual reset.

A.7.4 Operating Bypass

The operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing.

The operating bypasses have automatic features that provide a permissive range at which they can be actuated. Should the permissive range be exceeded, the bypass will be automatically removed.

A.7.5 Maintenance Bypass

One set of the redundant PPS Bistable Trip channels is bypassed for maintenance.

The protection functions of the RPS and ESFAS are maintained while the system is bypassed.

A.8 Power Source Requirements

A.8.1 Electrical Power Sources

The PPS and ESF-CCS channel receives non-interrupt AC power from VBPSS. The PPS power is provided with single phase 120 Vac from four independent A, B, C, D channel inverters. The ESF-CCS receives the single phase 120 Vac from four independent A, B, C, D channel inverters and 120 Vac from MCC Alternate sources.

A.8.2 Non-electrical power sources

This requirement is not applicable.

A.8.3 Maintenance Bypass

This requirement is not applicable.

APPENDIX B CONFORMANCE TO IEEE STD. 7-4.3.2-2003

This Appendix describes how the safety I&C systems satisfy the requirements of IEEE Std. 7-4.3.2-2003 endorsed by RG 1.152. The following heading numbers with "B" correspond to the section numbers of IEEE Std. 7-4.3.2-2003.

B.1 Scope

The computer based safety system criteria contained in IEEE Std. 7-4.3.2 are applicable to the safety I&C systems, which initiate safety actions to mitigate the consequences of DBE. It is also applicable to those parts of DCSs that support safety system functions.

B.2 References

The safety I&C systems conform to all referenced codes and standards.

B.3 Definitions and abbreviations

There is no exception in the safety I&C systems designs.

B.4 Safety System Design Basis

No requirements beyond IEEE Std. 603-1991 are necessary.

B.5 Safety System Criteria

B.5.1 Single-Failure Criterion

No requirements beyond IEEE Std. 603-1991 are necessary.

B.5.2 Completion of Protective Action

No requirements beyond IEEE Std. 603-1991 are necessary.

B.5.3 Quality

B.5.3.1 Software Development

The software quality assurance plan (SQAP) for the safety I&C systems application software is described in Section 5.3 of this report.

B.5.3.1.1 Software Quality Metrics

Software quality is assured through the application of a rigorous software life cycle process. The process covers software development (or qualification of COTS software), verification review and validation testing at the different stages of development, and software configuration management during all phases of software development. The use of software tools is controlled by the development process and meets the guidance set forth in IEEE Std. 7-4.3.2.

Throughout the project life cycle, a software requirements traceability analysis will be performed and a RTM maintained. The RTM lists all of the requirements discovered and traced in the V&V process.

B.5.3.2 Software Tools

The software development tools (e.g., application programming tool, requirements management tool, compiler, linker, etc) are placed under configuration management and classified as "general purpose".

The defects induced by software tool can be detected and removed through the comprehensive V&V and testing process described in Section 5.4 of this report.

B.5.3.3 Verification and Validation

The verification and validation for the safety I&C systems application software is described in Section 5.5 of this report.

B.5.3.4 Independent V&V Requirements

Independence of verification and validation for the safety I&C systems is described in Section 5.5 of this report.

B.5.3.5 Software Configuration Management

The software configuration management for the safety I&C systems is described in Section 5.6 of this report.

B.5.3.6 Software Project Risk Management

The SMP includes the software project risk management to identify and assess the risk factors associated with the system. All of the items that have an impact are listed in the SMP. And this impact is described with a method for a managing that risk.

- Financial risks
- Schedule risks
- Contractual risks
- Technology change risks
- Size and complexity risks
- Scale-up risks
- Work package (activities and tasks to be completed) unavailability risks

B.5.4 Equipment Qualification

B.5.4.1 Computer System Testing

The computer-based system testing process for the safety I&C systems is described in Section 5.4.e of this report.

B.5.4.2 Qualification of Existing Commercial Computers

The commercial dedication for the safety I&C systems is described in Section 5.7 of this report.

B.5.5 System Integrity

B.5.5.1 Design for Computer Integrity

The safety I&C systems are designed for fail-safe operation under component failure or loss of electrical power.

The safety I&C systems software integrity is assured by software development process and activities described in Section 5 of this report.

B.5.5.2 Design for Test and Calibration

All processor stations have self-diagnostics that continuously monitor the hardware modules and software functions. This diagnostic information is sent to the ITP/MTP FPD for display and alarm processing. The IPS monitors the process values and setpoint values received from for all channel ITPs. These features do not interfere with normal system operation.

Channels are maintained and calibrated in a bypassed condition without initiating a protective action at the system level. Lifting electrical leads or installing jumpers need not be done to accomplish this process. Periodic testing is permitted during power operation.

B.5.5.3 Fault Detection and Self-Diagnostics

Upon power-up, diagnostics are performed including processors, I/O and memory to confirm readiness of the safety I&C systems. A complete set of these diagnostics are executed during initialization. This will detect any fatal errors prior to execution of the process loop.

During initialization, the watchdog function remains in the actuated state. Upon completion of the initialization tests, the processors will start automatically and run. Upon entry to the run mode, the watchdog function will automatically reset to the non-actuated state. Processor operability is continuously tested in the run mode and the watchdog function is actuated upon detection of failure.

B.5.6 Independence

The methods used to ensure communication independence between different safety channels and safety and non-safety systems is described in Section 4.6 of this report. The methods include:

a. Electrical isolation

   Fiber optic cables are used for electrical isolation between computers in different safety channels or safety and non-safety computers. The fiber optic cables provide inherent isolation for electrical faults since it does not carry the electrical current.

b. Functional isolation

   The PM employs independent communication section (CS) that is separate from the processing section (PS) that performs safety functions. The PS and CS communicate via dual ported memory using 'Broadcast' philosophy. Communication data is not transferred by the PS unless specifically configured within the application program. This ensures there is no potential for communications functions to disrupt deterministic safety function processing.

c. Communication isolation

   One way communication with 'Broadcast' philosophy is used for communication isolation.

d. No ability to transfer unpredicted data

There is no event driven programming in the safety I&C systems. Only predefined communication data set are transferred between safety channels and from safety to non-safety computers at the fixed interval.

e. No ability to alter safety software

The software in the safety I&C systems cannot be changed through the communication interface between the redundant channels or the communication interface for the Control and Monitoring System. The safety I&C systems software (e.g., setpoint) is changeable only through the Maintenance and Test Panel within the same channel.

B.5.7 Capability for Test and Calibration

No requirements beyond IEEE Std. 603-1991 are necessary.

B.5.8 Information Displays

No requirements beyond IEEE Std. 603-1991 are necessary.

B.5.9 Control of Access

No requirements beyond IEEE Std. 603-1991 are necessary.

B.5.10 Repair

No requirements beyond IEEE Std. 603-1991 are necessary

B.5.11 Identification

All software and documentation will be uniquely identified by a system name, number, and corresponding revision date, appropriate category and software classification as described in Section 5.6.

The configuration Items referenced and controlled by the SCMP are as follows:

- Operating System including Compiler and Linker
- Run time source and executable files
- Associated Software Documents

B.5.12 Auxiliary Features

No requirements beyond IEEE Std. 603-1991 are necessary.

B.5.13 Multi-Unit Stations

No requirements beyond IEEE Std. 603-1991 are necessary.

B.5.14 Human Factor Considerations

No requirements beyond IEEE Std. 603-1991 are necessary.

B.5.15 Reliability

The reliability analysis method for the safety I&C systems is described in Section 7 of this report.

B.6 Sense and Command Features – Functional and Design Requirements

No requirements beyond IEEE Std. 603-1991 are necessary.

B.7 Execute Features – Functional and Design Requirements

No requirements beyond IEEE Std. 603-1991 are necessary.

B.8 Power Source Requirements

No requirements beyond IEEE Std. 603-1991 are necessary.

APPENDIX C CONFORMANCE TO ISG-04

TS

C.1 Scope

C.2 References

TS

C.3 Data Communication Systems

TS

Figure C.3-1 Data Communication System

TS

C.4 System Descriptions

TS

TS

C.5 Compliance Analysis to Criteria

C.5.1 Inter-channel Communications

TS

TS

TS

TS

TS

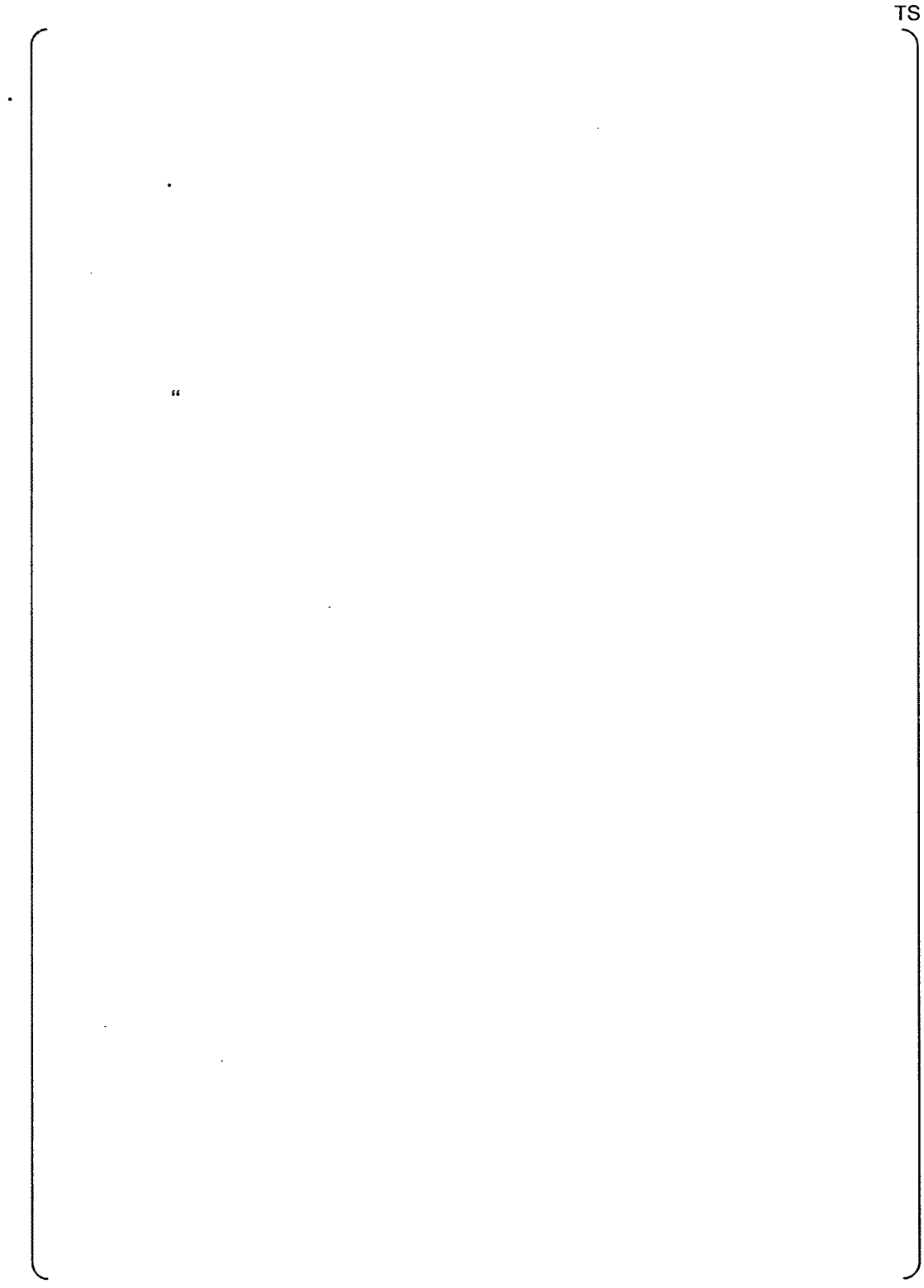
TS

TS

TS

TS

TS



TS

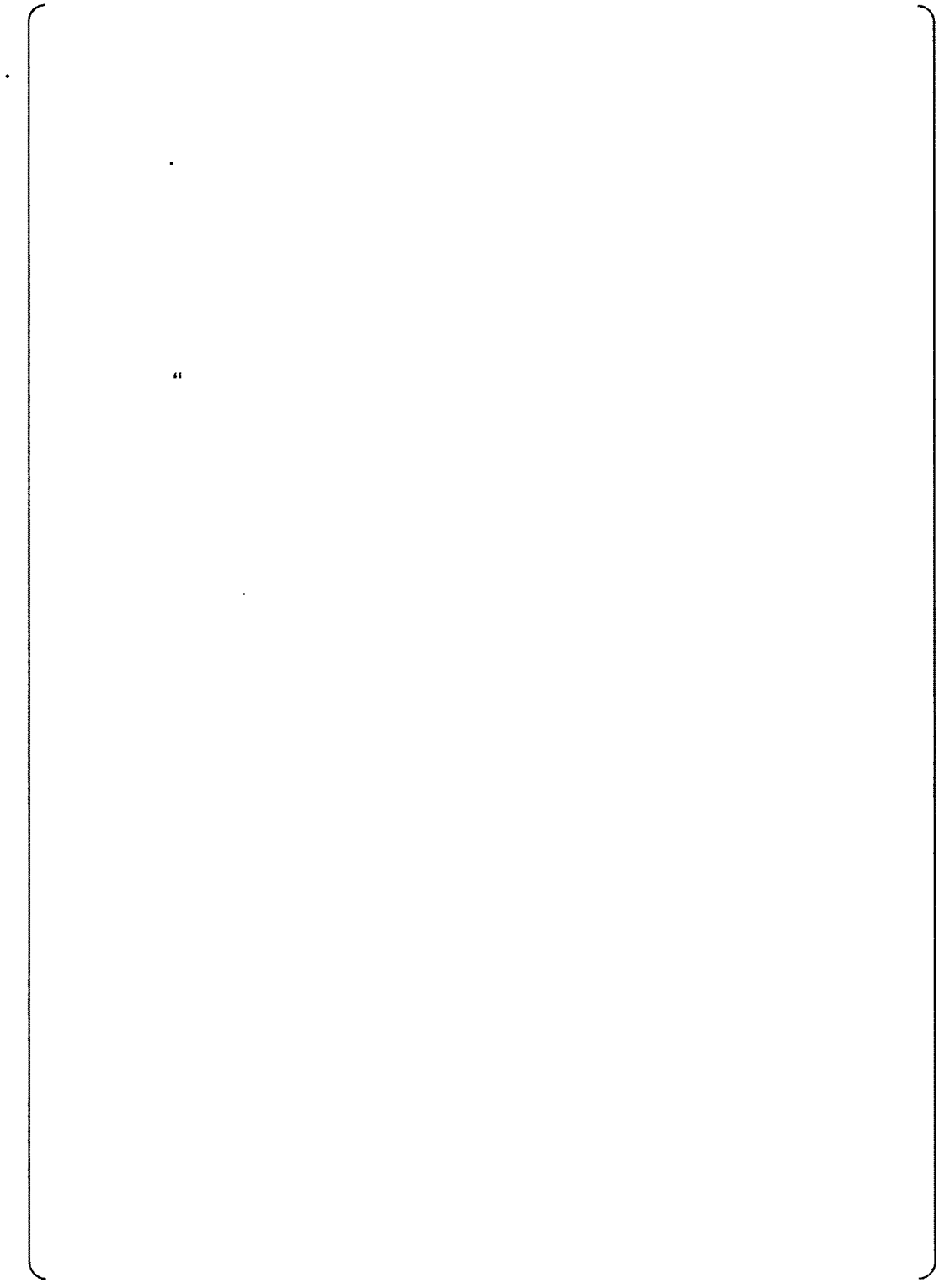
TS

TS

TS

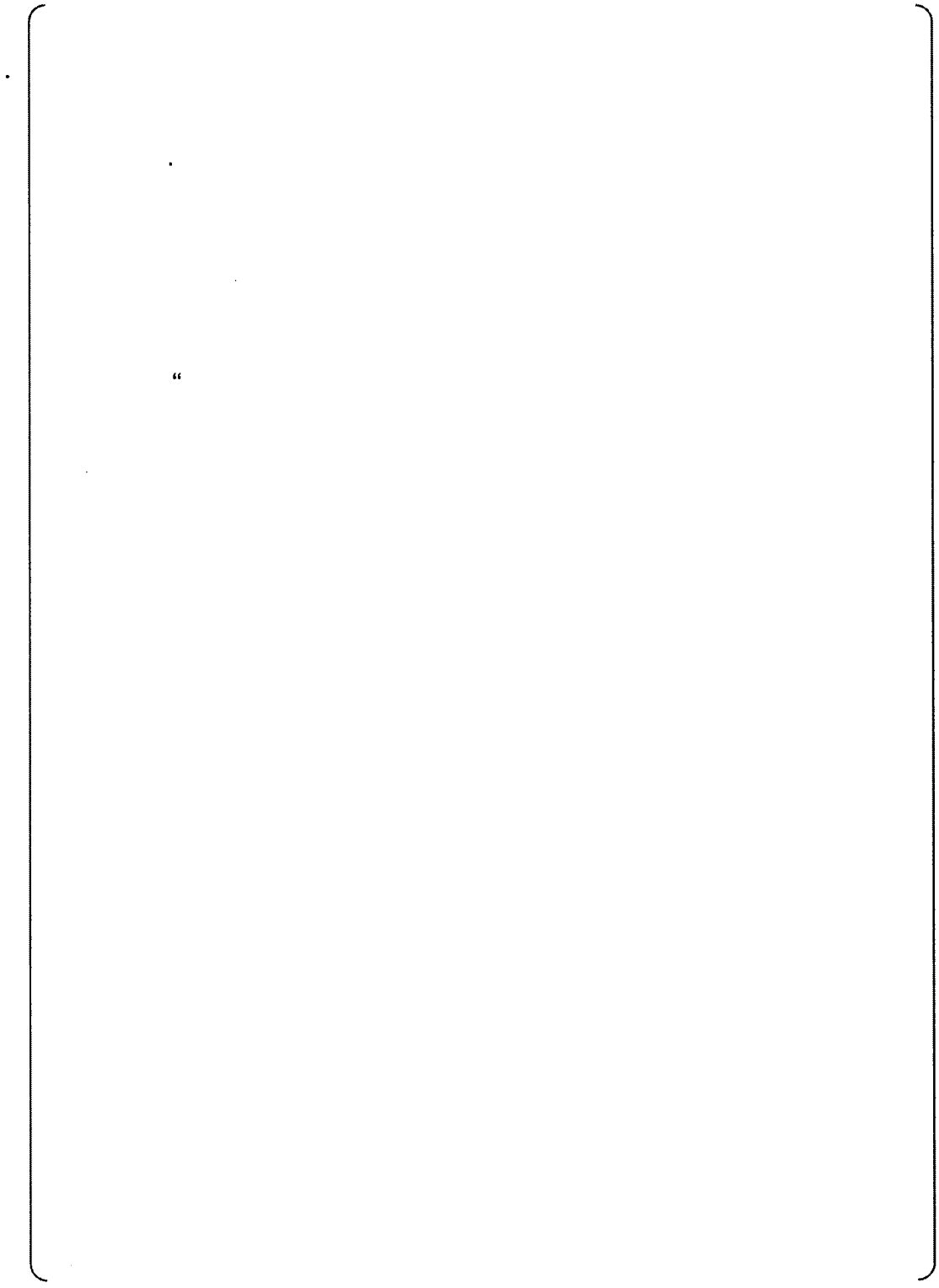
TS

TS



TS

TS



TS

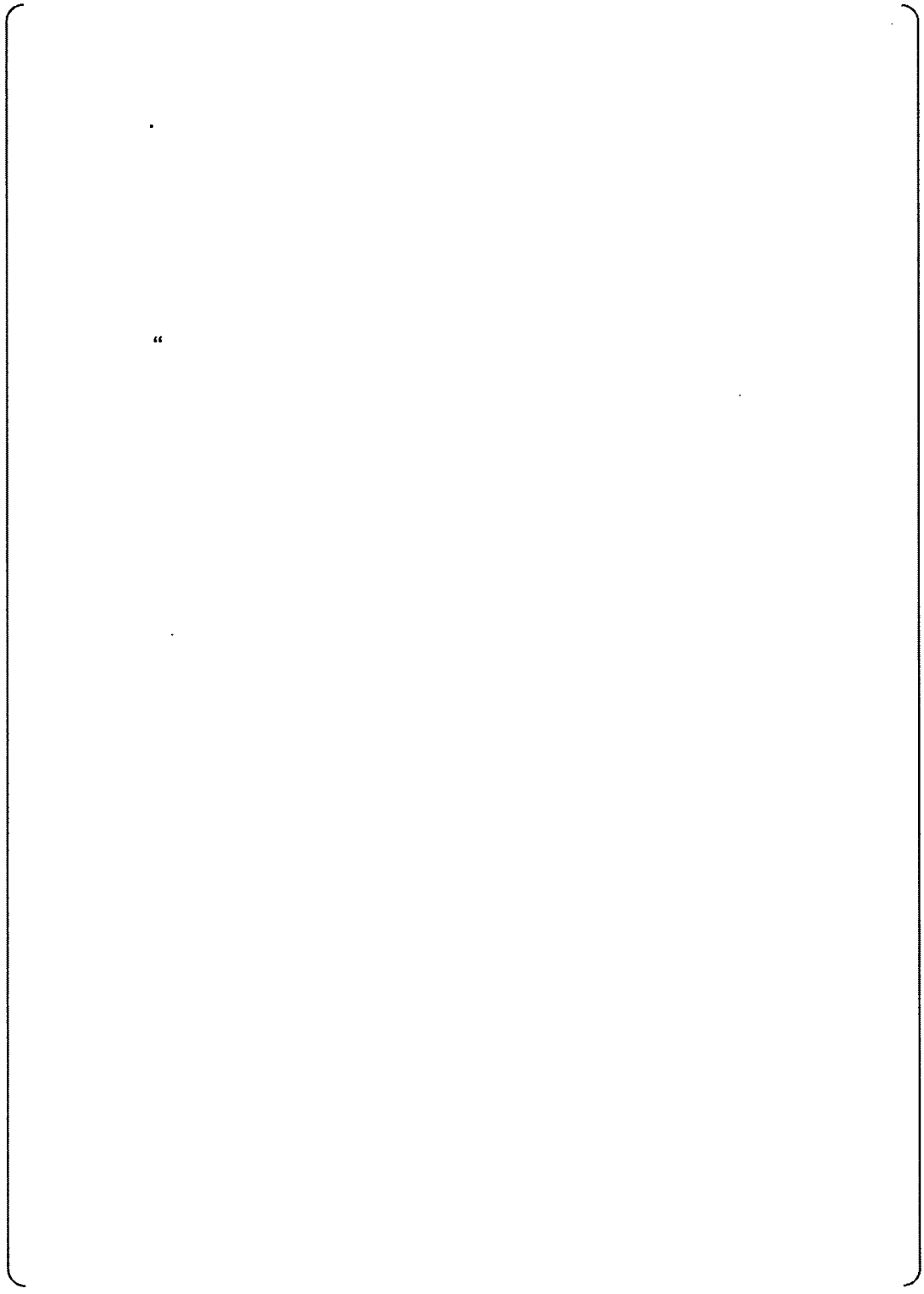
TS

Table C.5.1-1 RSPT1 and RSPT2 Channel Assignment

"

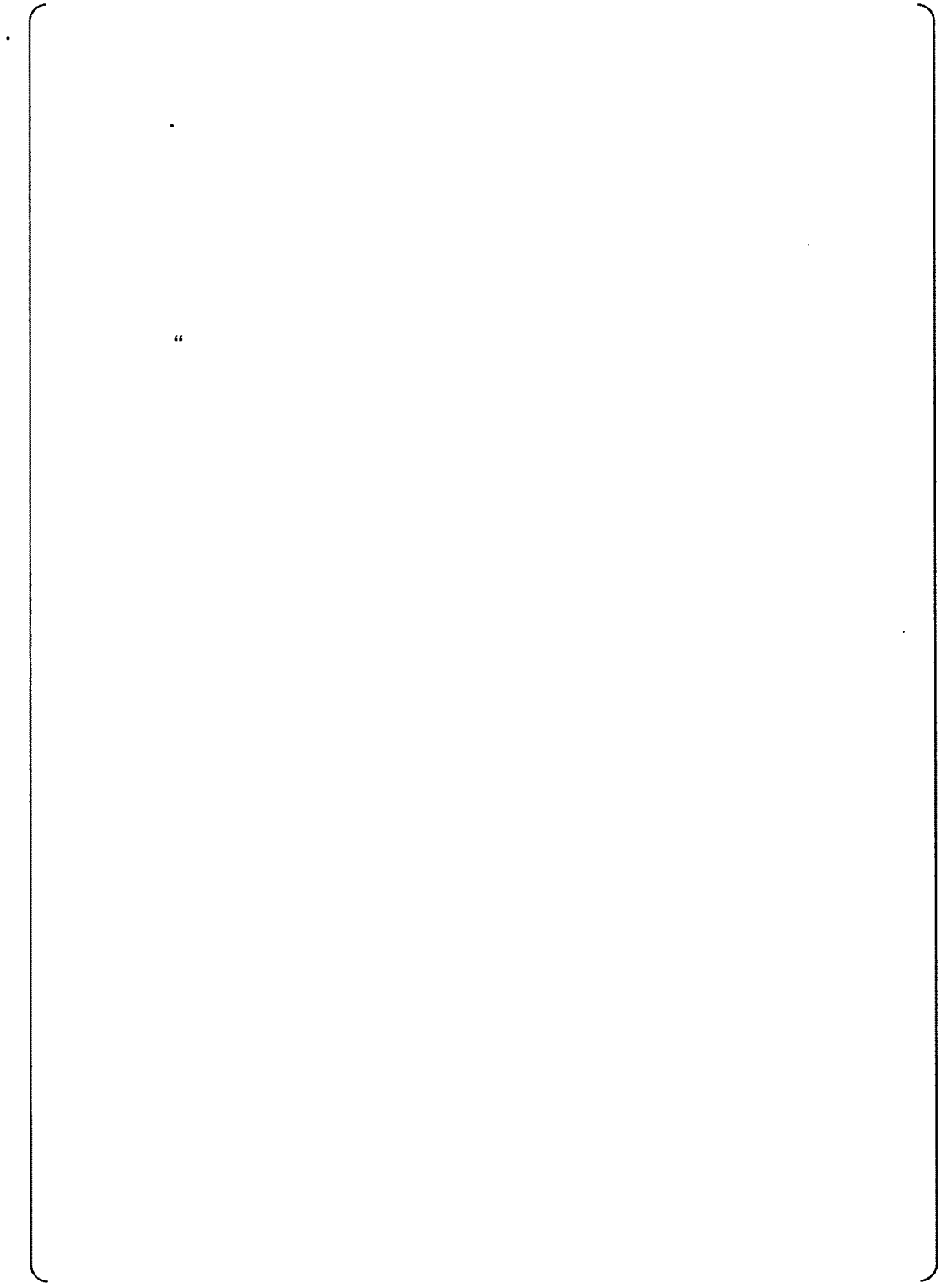
TS

TS



TS

TS



TS

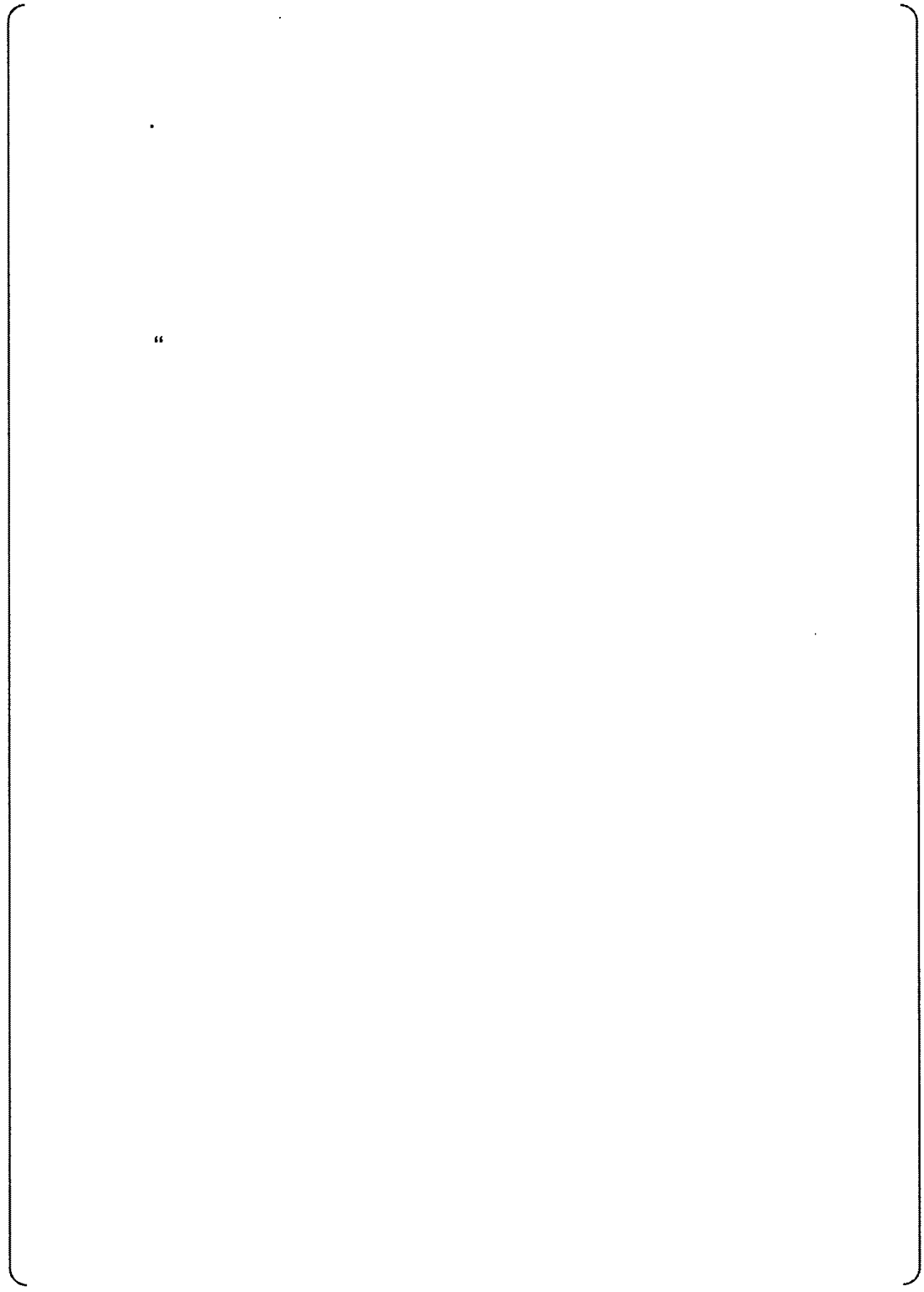
TS

TS

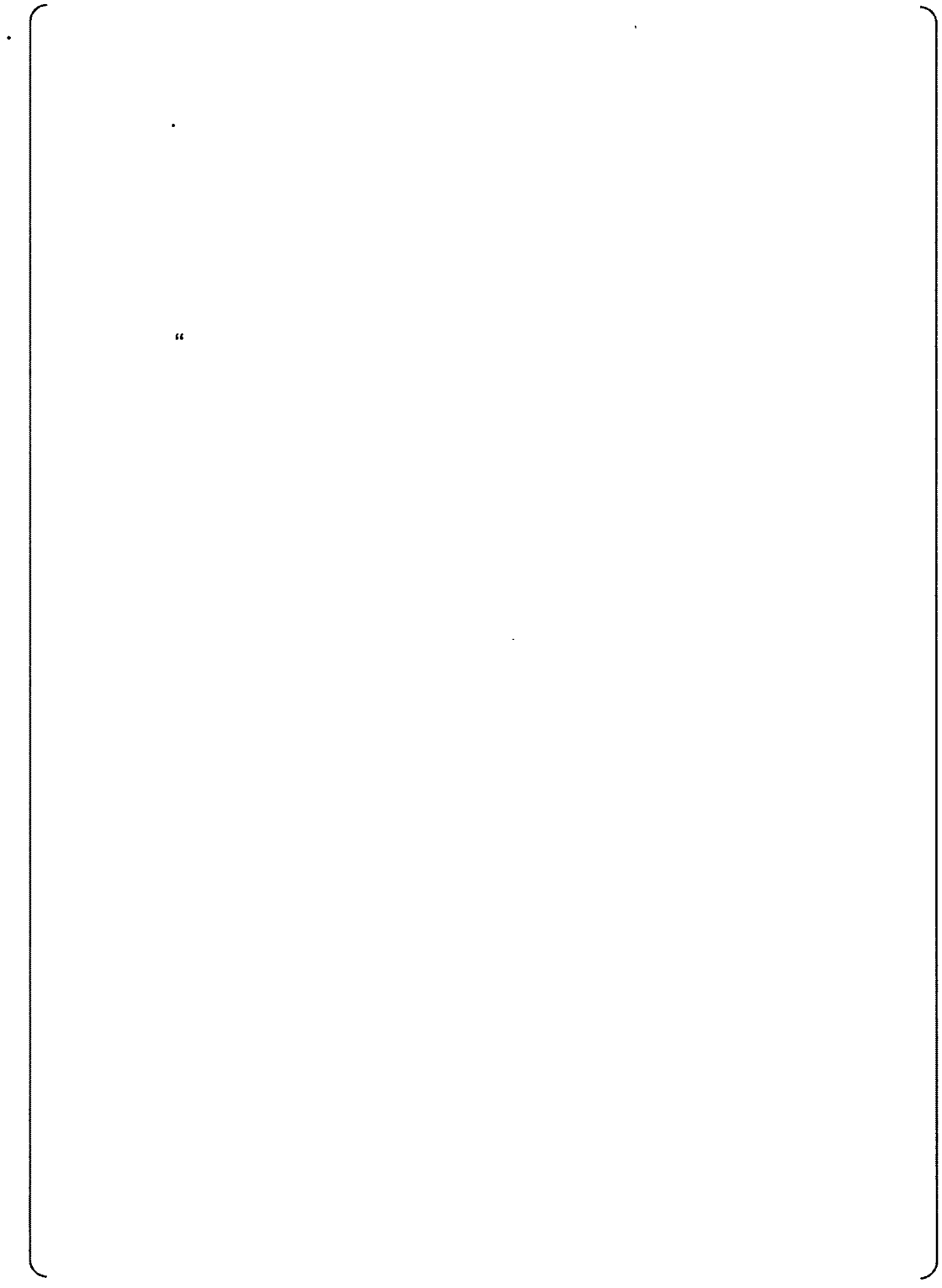
TS

TS

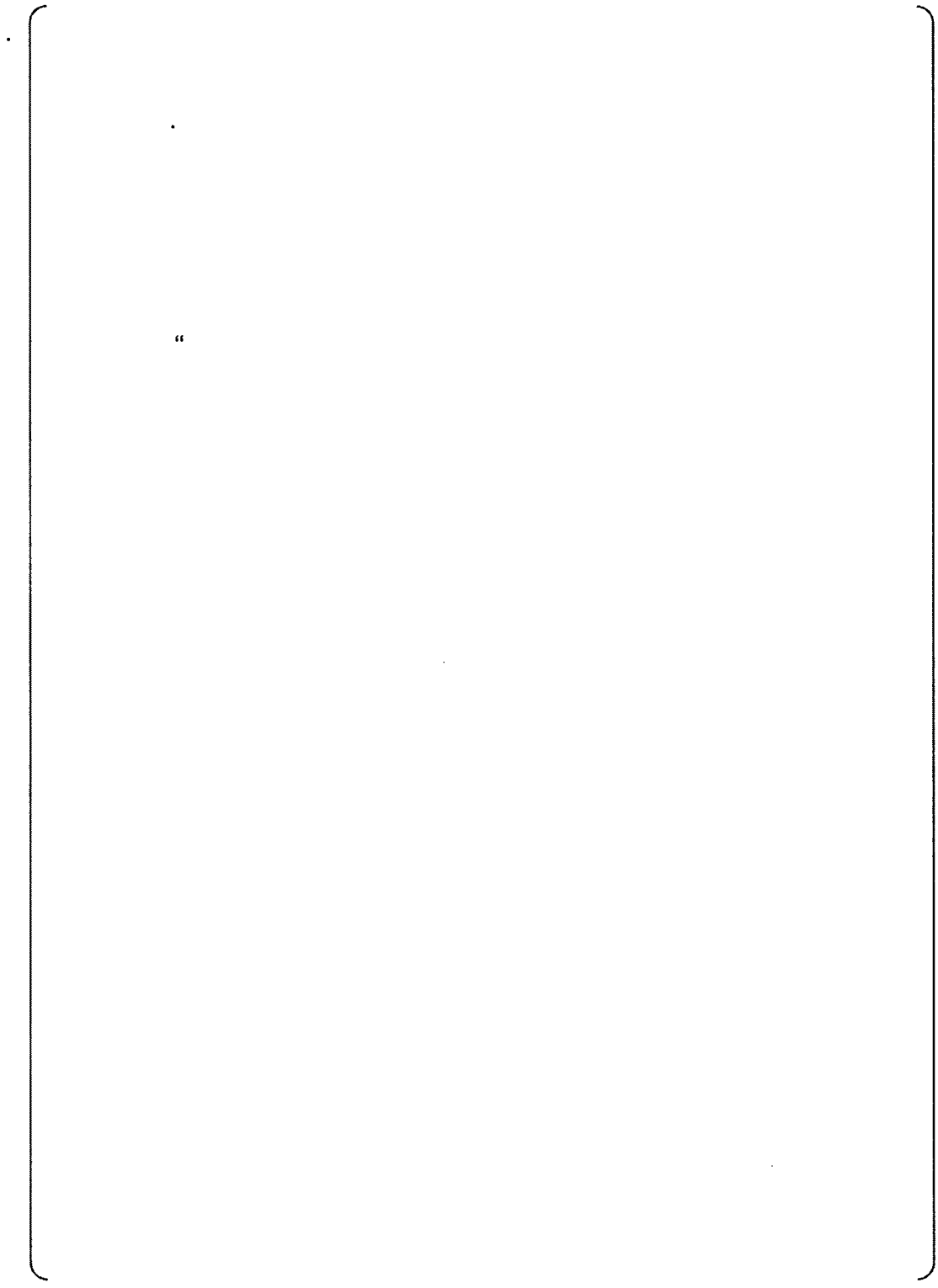
TS



TS

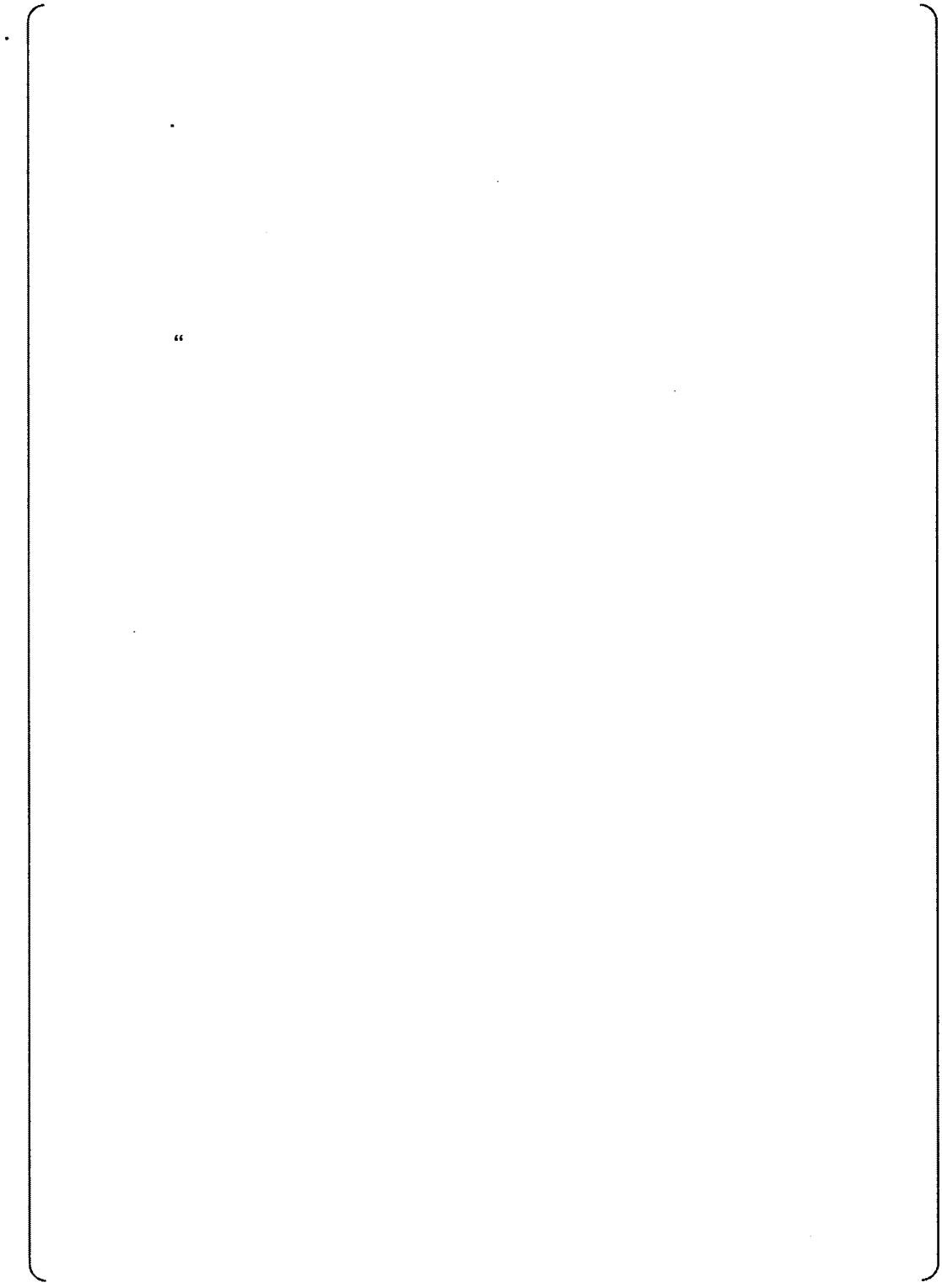


TS



TS

TS



[redacted]

KEPCO

KHNP